SAAD DAHLAB UNIVERSITY
Faculty of science
In Informatic Department

DOCTORAL THESIS

Speciality: Information Systems Security

SECURITY BY CONSTRUCTION THROUGH FORMAL METHODS AND BLOCKCHAIN: APPLICATION ON IOT NETWORKS IN SMART CITIES

By

Walid MILOUD DAHMANE

before the jury composed of:

M. Ould Khaoua	Professor, Blida 1 University	President
H. Bouarfa	Professor, Blida 1 University	Rapporter
S. Ouchani	A.Professor, CESI, France	Co. Director
N. Boustia	Professor, Blida 1 University	Examiner
D. Bennouar	Professor, Bouira University	Examiner
M. Brahmia	A.Professor, CESI, France	Examiner

Blida, May 2023

Declaration of Authorship

I, Walid MILOUD DAHMANE, declare that this thesis titled, “Security by Construction through Formal Methods and Blockchain: Application on IoT Networks in Smart Cities” and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.

Signed:

Date:

“*When you’re a carpenter making a beautiful chest of drawers, you’re not going to use a piece of plywood on the back, even though it faces the wall and nobody will see it. You’ll know it’s there, so you’re going to use a beautiful piece of wood on the back. For you to sleep well at night, the aesthetic, the quality, has to be carried all the way through.* ”

Steve Jobs

“*Try not to become a man of success. Rather become a man of value.* ”

Albert Einstein

Abstract

Since ancient times, people have believed that the city is a symbol of civilization and development, as it was a pioneer in adopting modern technical means. With the immense increase of population density in cities, many challenges face citizens and governments. Thus, it has become mandatory to convert our cities to be smart. Currently, the world is witnessing a revolution in the technical field, wherewith the emergence of Information and Communication Technologies (ICT), the Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, and other modern information technologies, the treating of data has become more effective than before. Modern Smart cities require Building Information Models (BIM) and a scalable system that allow easy access and efficient analysis of information for better management of the smart city. The sustainability of the smart city depends on the safety of its digital world from internal and external dangers, by guarantying the integrity of information and the control access system. This thesis deals with the issue of protecting the city through blockchain technology, as it has passed through multiple stages, namely, we tried hard to support smart cities researchers with abundant and reliable information, which focused on the spread and use of IoT, the important aspects of the smart city (such as the advantages, applications, and challenges), and the service evaluation methodology through calculating requests and responses. Moreover, the information was presented sequentially and simplified. we developed a methodology that systematically builds a reliable and secure Smart City Model (SCM) that can be integrated within the building information model (BIM). SCM encloses both physical and digital models which are deployed smart buildings in particular. To optimize the deployment of nodes in the smart area, the ISOD framework built a multi-objective evolutionary optimization algorithm, exploits BIM database information including the physical properties of the used materials in the obstacles, and deploys dynamically the optimal WSN configuration. To enhance the security level of the smart city system, we propose a two-layer framework based on blockchain technology. In the first step, we develop a blockchain architecture to be the mainstay for protecting all types of information that is collected by smart devices within a smart city. In the second step, we create an access control system named SOT-S (Subject-Object-Task System) supported by the blockchain technology that sorts out the access processes applied by subjects on these smart devices. In the application and verification step, with the SCM, we used Cooja network simulators and Uppaal model checker to ensure the ability to apply our proposition on reality. Also, the effectiveness of ISOD has been shown on different scenarios and the results showed that ISOD deployments have maximum coverage with reliable connectivity. In addition, we implemented a test environment that integrates the proposed layers based on blockchain, where, it shows the effectiveness of both of them.

ملخص

منذ القدم ، كان الناس يعتقدون أن المدينة هي رمز الحضارة والتطور ، حيث كانت رائدة في تبني الوسائل التقنية الحديثة. مع الزيادة الهائلة في الكثافة السكانية في المدن ، يواجه المواطنون والحكومات العديد من التحديات. وبالتالي ، أصبح من الضروري تحويل مدننا إلى مدن ذكية. يشهد العالم حاليًا ثورة في المجال التقني ، مع ظهور تقنيات المعلومات والاتصالات، إنترنت الأشياء ، الذكاء الاصطناعي ، الحوسبة السحابية ، وغيرها من تقنيات المعلومات الحديثة، معالجة البيانات أصبحت أكثر فعالية من ذي قبل. تتطلب المدن الذكية الحديثة نماذج معلومات البناء (BIM) ونظامًا قابلًا للتطوير يتيح سهولة الوصول والتحليل الفعال للمعلومات من أجل إدارة أفضل للمدينة الذكية. تعتمد استدامة المدينة الذكية على سلامة عالمها الرقمي من الأخطار الداخلية والخارجية ، من خلال ضمان سلامة المعلومات ونظام التحكم في الوصول. تتناول هذه الرسالة موضوع حماية المدينة من خلال تقنية blockchain ، حيث مرت بمراحل متعددة وهي: حاولنا جاهدين دعم باحثي المدن الذكية بمعلومات وفيرة وموثوقة ، والتي ركزت على انتشار واستخدام إنترنت الأشياء ، والجوانب المهمة للمدينة الذكية (مثل المزايا والتطبيقات والتحديات) ، ومنهجية تقييم الخدمة من خلال حساب الطلبات والاستجابات. علاوة على ذلك ، تم تقديم المعلومات بشكل تسلسلي ومبسط. لقد طورنا منهجية تقوم بشكل منهجي ببناء نموذج مدينة ذكية موثوق وآمن (SCM) يمكن دمجه في نموذج معلومات المبنى (BIM). SCM يتضمن كلاً من النماذج المادية والرقمية التي تكون منتشرة على المباني الذكية على وجه الخصوص. لتحسين نشر العقد في المنطقة الذكية ، قام إطار العمل ISOD ببناء خوارزمية تحسين تطورية متعددة الأهداف ، واستغلال معلومات قاعدة بيانات BIM بما في ذلك الخصائص الفيزيائية للمواد المستخدمة في العوائق ، ونشر النموذج الأمثل لشبكات WSN بشكل ديناميكي. لتعزيز مستوى الأمان في نظام المدينة الذكية ، نقترح إطار عمل من طبقتين يعتمد على تقنية blockchain ، في الخطوة الأولى ، نقوم بتطوير بنية blockchain لتكون الدعامة الأساسية لحماية جميع أنواع المعلومات التي يتم جمعها بواسطة الأجهزة الذكية داخل المدينة الذكية. في الخطوة الثانية ، أنشأنا نظامًا للتحكم في الوصول باسم SOT-S مدعومًا بتقنية blockchain التي تنتقي عمليات الوصول التي يطبقها المستخدمون على هذه الأجهزة الذكية. في مرحة التطبيق و التحقق، فيما يتعلق بالنموذج SCM ، استخدمنا مدقق نموذج Cooja و Uppaal لضمان القدرة على تطبيق اقتراحنا على الواقع. كما تم عرض فعالية ISOD في سيناريوهات مختلفة وأظهرت النتائج أن عمليات نشر ISOD لها أقصى تغطية مع موثوقية الاتصال. بالإضافة إلى ذلك ، قمنا بتنفيذ بيئة اختبار تدمج الطبقات المقترحة مبنية على blockchain ، حيث تظهر فعالية كل منهما.

Résumé

Depuis l'Antiquité, les gens croient que la ville est un symbole de civilisation et de développement, car elle a été pionnière dans l'adoption des moyens techniques modernes. Avec l'immense augmentation de la densité de population dans les villes, de nombreux défis se posent aux citoyens et aux gouvernements. Ainsi, il est devenu obligatoire de convertir nos villes en smart. Actuellement, le monde assiste à une révolution dans le domaine technique, avec l'émergence des technologies de l'information et de la communication (TIC), de l'Internet des objets (IoT), de l'intelligence artificielle (IA), du cloud computing et d'autres technologies de l'information modernes, le traitement des données est devenu plus efficace qu'auparavant. Les villes intelligentes modernes nécessitent des modèles d'information sur le bâtiment (BIM) et un système évolutif qui permettent un accès facile et une analyse efficace des informations pour une meilleure gestion de la ville intelligente. La pérennité de la ville intelligente passe par la sécurité de son monde numérique vis-à-vis des dangers internes et externes, en garantissant l'intégrité des informations et le système de contrôle d'accès. Cette thèse traite de la question de la protection de la ville grâce à la technologie blockchain, car elle est passée par plusieurs étapes, à savoir, nous nous sommes efforcés de soutenir les chercheurs sur les villes intelligentes avec des informations abondantes et fiables, axées sur la diffusion et l'utilisation de l'IoT, les aspects importants de la ville intelligente (tels que les avantages, les applications et les défis) et la méthodologie d'évaluation des services en calculant demandes et réponses. De plus, les informations étaient présentées de manière séquentielle et simplifiée. nous avons développé une méthodologie qui construit systématiquement un modèle de ville intelligente fiable et sécurisé (SCM) qui peut être intégré dans le modèle d'information du bâtiment (BIM). Le SCM renferme à la fois des modèles physiques et numériques qui sont notamment déployés dans les bâtiments intelligents. Pour optimiser le déploiement des nœuds dans la zone intelligente, le cadre ISOD a construit un algorithme d'optimisation évolutif multi-objectifs, exploite les informations de la base de données BIM, y compris les propriétés physiques des matériaux utilisés dans les obstacles, et déploie dynamiquement la configuration WSN optimale. Pour améliorer le niveau de sécurité du système de ville intelligente, nous proposons un cadre à deux couches basé sur la technologie blockchain. Dans la première étape, nous développons une architecture blockchain pour être le pilier de la protection de tous les types d'informations collectées par les appareils intelligents au sein d'une ville intelligente. Dans la deuxième étape, nous créons un système de contrôle d'accès nommé SOT-S (Subject-Object-Task System) pris en charge par la technologie blockchain qui trie les processus d'access appliqués par les sujets sur ces appareils intelligents. Dans l'étape d'application et de vérification, avec le SCM, nous avons utilisé le simulateur de réseau Cooja et le vérificateur de modèle Uppaal pour garantir la capacité d'appliquer notre proposition à la réalité. De plus, l'efficacité de l'ISOD a été démontrée sur différents scénarios et les résultats ont montré que les déploiements ISOD ont une couverture maximale avec des connectivité. En outre, nous avons mis en place un environnement de test qui intègre les couches proposées basées sur la blockchain, où, il montre l'efficacité des deux.

Acknowledgements

Throughout the writing of this dissertation I have received a great deal of support and assistance.

I would first like to thank my supervisor, Doctor Samir Ouchani, whose expertise was invaluable in formulating the research questions and methodology. Your insightful feedback pushed me to sharpen my thinking and brought my work to a higher level.

Professor Hafida Bouarfa was my teacher before she was my supervisor, I learned a lot from her, and she did not skimp on me with requests.

I would be remiss in not mentioning the present Pr.Mohamed Ould khaoua, and jury members Pr. Narhimene Boustia, Pr. Djamel Bennouar, and Dr. Mohamed Amine Brahmia.

Big thanks to my classmates, especially Mohamed Ramla and Omar Legouati, I had a very interesting time with them.

I will not forget my parents who supported me financially and morally throughout my academic career. Also all my family members who shared my joy and my hard times.

Contents

List of Figures

List of Tables

List of Abbreviations

SC	**S**mart **C**ity
IoT	**I**nternet **o**f **T**hings
CPS	**C**yber **P**hysical **S**ystem
ISOD	**I**ndoor **S**ensor **O**ptimal **D**eployment **F**ramework
BIM	**B**uilding **I**nformation **M**odel
ICT	**I**nformation and **C**ommunication **T**echnologies
IA	Artificial **I**ntelligence
SCM	**S**mart **C**ity **M**odel
WSN	**W**ireless **S**ensor **N**etwork
SOT-S	**Subject**-**O**bject-**T**ask **S**ystem
ITS	**I**ntelligent **T**ransportation **S**ystems
PM	**P**hysical **M**odel
DM	**D**igital **M**odel
SH	**S**mart **H**ome
SR	**S**mart **R**oom
TCTL	**T**imed **C**omputation **T**ree **L**ogic
BC	**B**lock**C**hain
RSA	**R**ivest **S**hamir **A**dleman
SSL	**S**ecure **S**ockets **L**ayer
MQTT	**M**essage **Q**ueuing **T**elemetry **T**ransport
TLS	**T**ransport **L**ayer **S**ecurity
ACM	**A**ccess **C**ontrol **M**odel
RPL	**R**outing **P**rotocol for **L**ow-Power and Lossy Networks

6LoWPAN	IPv**6** over **Lo**w-Power **W**ireless **P**ersonal **A**rea **N**etworks
CoAP	**Co**nstrained **A**pplication **P**rotocol
AMQP	**A**dvanced **M**essage **Q**ueuing **P**rotocol
DTLS	**D**atagram **T**ransport **L**ayer **S**ecurity
KPI	**K**ey **P**erformance **I**ndicators
SHA	**S**ecure **H**ash **A**lgorithm
ML	**M**achine **L**earning
DL	**D**eep **L**earning

I dedicate this work to my first support, my parents, who were keen on my upbringing and education more than they were concerned about themselves. I do not forget all my family members. Special thanks to my supervisors who had the most prominent role in completing my work.

Chapter 1

General Introduction

UNESCO[1] stated that through innovative urban systems, smart cities play an important role in socio-economic development while improving people's lives [1]. As defined by UNECE[2], a sustainable smart city is an innovative city that uses ICTs (Information and Communication Technologies) to enhance the quality of life, the efficiency of urban operations, and competitiveness [2]. A smart city [3–5] is a city that consists of a lot of intelligent components, such as smart buildings, smart health, smart ICTs, smart grids, smart transportation, and more [6].

1.1 Motivations

There are many motives that encourage us to develop smart cities. In the following examples, we will present some facts that demonstrate the impact of the Internet of Things devices, machine learning, and big data in improving the lives of citizens within smart cities. We can exploit the features of IoT devices for several useful purposes, for example, smart objects have a positive impact on organizations as it allows process automation, optimize service delivery, and transfer data to the computing cloud [7]. In addition, smart devices in a smart city can improve the health sector, where the smart city can help us to continue in this condition due to the announcement of the Coronavirus spread [8]. A

[1] United Nations Educational, Scientific and Cultural Organization.

[2] United Nations Economic Commission for Europe.

comparison has been made to know the performances of Cloud, Fog, Mist, and Edge computing for IoT systems, despite the efforts made to connect them, but they were hollow due to the difficulty of achieving reliable systems [9], these architectures give the system protection, fast data-flow, and high storage spaces, which encourages its integration into the system.

Embedded technology encourages developers to build a secure system, where IoT infrastructure, artificial intelligence, big data, IoT, mobile Internet, cloud computing, management, and urban planning have a key role in the integration of smart cities [10]. Also, Big data collected from different sectors such as healthcare, IoT devices, and enterprises have attributes. The topic of machine learning (ML) is widespread and can be exploited in the concept of the smart city, for example, ML algorithms are used to detect patterns, and they can be used for potential predictions, this helps medical practitioners and people at the managerial level to make decisions [11], future expectations help to avoid mistakes and reduce material and human losses. Another motive. Big data and the Internet of Things can turn the idea of a smart city into a reality [12]. The transportation sector is also developing, where traditional transportation systems seek to optimize resources, in addition to being able to meet the expectations of stakeholders, so, for high-density cities to manage traffic and use resources reliably, they rely on Intelligent Transportation Systems (ITS) [13]. Among the benefits of a smart city, we mention, improving the quality of life of its inhabitants, commuting workers and students, and other visitors, in addition, significantly improving its resource efficiency, decreasing its pressure on the environment, and increasing resiliency, also, building an innovation-driven, green economy, and fostering a well-developed local democracy [14].

Gartner's curve of 2021 (Figure 1.1) shows the hype cycle for emerging technologies. The curve indicates the emergence of *decentralized finance* technology, this latter does not depend on a third party to manage the banking transactions, users are the ones who process transactions with the presence of a document that proves the validity of the transactions applied. Digital currencies (such as Bitcoin) use this technology, Bitcoin relies on blockchain technology, which was the main reason for protecting transactions, and cracking the protection of the blockchain system is almost impossible. Thus, the technology has been in great demand, as a result, the value of Bitcoin is currently hundreds of times greater than cash (such as the dollar). Depending on the *Gartner* curve, the technology will expand after 5 to 10 years.

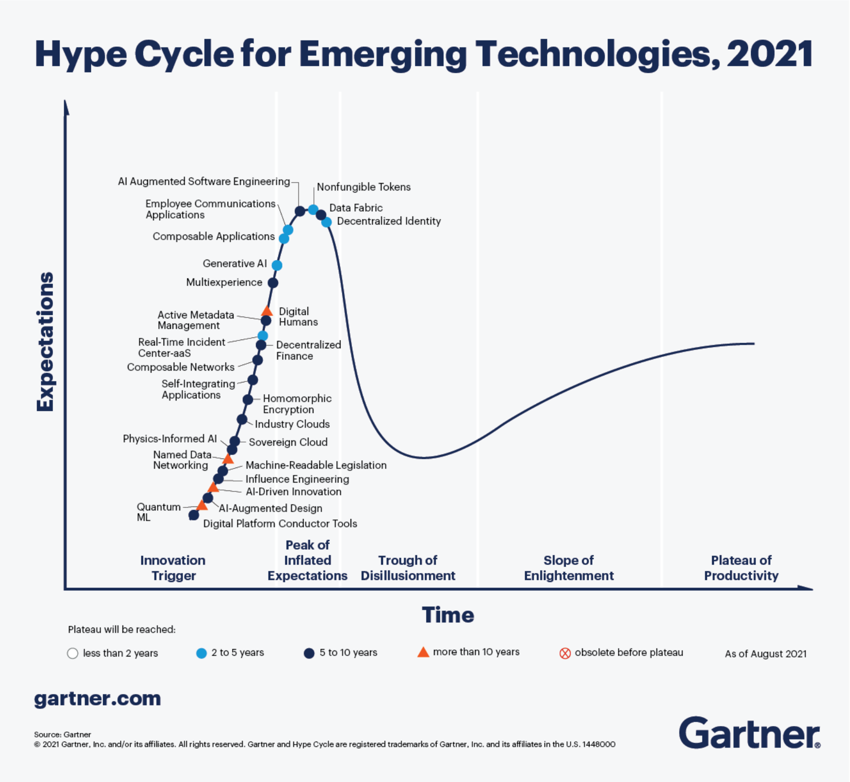


FIGURE 1.1: Hype Cycle for Emerging Technologies, 2021 [15].

1.2 Problem statements

Many contributions describe the components of the smart city [16–18] as collections of smart buildings, smart transportation, smart ICT, smart health, smart infrastructure, smart economy, and smart government. However, the increasing population in the cities during the last years has resulted in many challenges like great energy consumption, management difficulty of big data, covering more areas with high-quality connection, dealing with emergencies in the buildings, protecting digital data from the collapse of the information system or hackers, transportation management, waste management, etc. These challenges cost the government a substantial amount of losses. To mitigate these problems, many recent projects are funded as shown in Table 1.1 [19].

City and Country	Population	Solutions	Major partners	Challenges
Busan - South Korea	3.4 million	Safety service for children/elderly, drone-based smart marine, smart parking, crosswalk, and energy usage	Busan government, Cisco, ETRI, KETI, SK Telecom, KT	- Approximate investment of US $452 million. - Deliver an improved transportation system. - Achievement e-healthcare services. - Increased jobs and business opportunities. - Improved information accessibility.
Santander - Spain	0.1 million	Smart metering of temperature, traffic intensity, humidity, transportation plans, water needs, etc.	Ericsson, Telefonica, Telefonica I+D	- Managing 15 big participants companies. - Recording the transmitted data collected by 20000 smart IoT devices. - Compiling the sensor data into a big picture.
Chicago United States	2.7 million	Smart grid, smart living, emergency alert, reduced crime	Cisco, IBM, Chicago government	- It Controls 300000 smart IoT devices. - It aims to reduce energy waste to save customers US$170 million. - Model has 31 variables to prevent rodent infestations.
Milton Keynes - United Kingdom	0.2 million	Smart transportation, reduced carbon emission, smart energy, water management	Milton Keynes Council, Samsung, Huawei, CATAPULT, Cambridge University	- Controlling carbon emissions and supporting sustainable growth without deploying additional infrastructure. - Resolving more issues like business, education, and community engagement activities.

TABLE 1.1: Smart city projects [19].

To motivate the trend towards a smart city, Table 1.2 shows the difference between traditional and smart cities. The comparison leads us to conclude that the smart city overcomes many of the problems faced by the current traditional cities. Based on this comparison, we realize that we must convert the actual cities to be smarter by deploying robust and secure components, and respecting security policies and smart city norms. This thesis seeks to cover and solve the following issues.

1. How do the formal methods represent systems, therefore guaranteeing their robustness?
2. How the components of a smart city are modeled?
3. What is the correct way to model, formalize, and validate the components of smart buildings?
4. How to ensure the correctness of a smart city?
5. How to secure a smart city?
6. How to optimize the deployment of the connected components in a smart city/ building?
7. How can we use formal methods to define the system, and the blockchain to ensure integrity and access control?

1.3 Challenges

The primary system is inherited and traditional, operating in a cumbersome and unreliable manner, in addition to failing to share information effectively, but with the development, deep application, cooperation of recent concepts and technologies presented by IoT, and cloud computing in the world of information, life has witnessed modernity and intelligence, all of which smart cities have gradually adopted [54]. Big data is one of the most important reasons for development in the field of information, where data is mined, analyzed, and shared [55]. The data is collected by the devices distributed on the buildings, roads, factories, schools, etc., after the analysis process, the city's condition can be assessed and the necessary measures are taken. The global cyber system is responsible for their identification, protection, routing, translation, and other processing to ensure a safe and reliable flow. Smart city technologies such as transportation and waste management are taken into consideration, unlike innovations related to security and crime prevention [56], the presence of security and stability among the population encourages continuity and vice versa. The city suffers from many problems related to energy, transportation, environment, protection, etc (Figure 1.2). The scary thing is that the problems are increasing over time due to the mockery of the citizens or the government does not have the required capacities.Table 1.3 presents challenges in European cities, which are related to affecting government, economy, mobility, environment, people, and living. Neglecting them leads to deteriorating conditions and the creation of a difficult area to live.

Regrettably, the world suffers from constant threats that affect the integrity of the information distributed in the city and particularly in the smart city. The appropriation of sensitive information such as election results and false promotions before the elections by foreign countries may push the target countries to become a colony.

There are many false stories on Internet sites that aim to increase advertising sales [64], the politicians spread misinformation during the 2009 healthcare debate [65], so, the smart city information is the result of unknown people, which forces us to collect them within a safe and reliable system. We believe that the reason for penetrating the systems they have is to test protection while penetrating the systems they do not have is for the purpose of espionage. We conclude that, the databases should be encrypted with a hard-to-crack technology that guarantees users' privacy, it is also required that the communication channels must be protected by protocols in order to avoid the sniffing attacks [66] which aim to steal the information and encryption keys.

The security tree in Figure 1.3 illustrates the importance of basic security requirements. The challenges specified at the root have to be addressed properly, just as the root secures the tree in the soil. When these basic requirements are met appropriately, the security tree ensures yields of benefits in terms of anything/everything as a Service

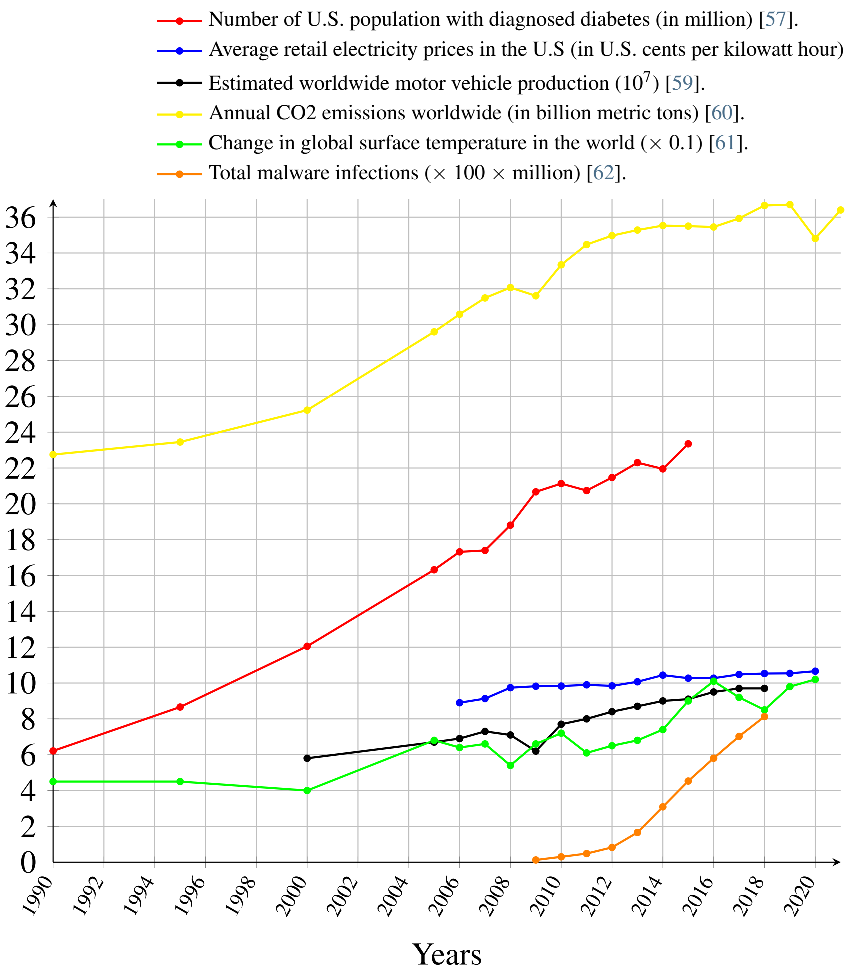


FIGURE 1.2: Smart Cities Challenges.

(XaaS), metaphorically depicted as the fruits/leaves in a tree. The Protocols (TLS) and (SSL) which are Transport Layer Security and Secure Socket Layer respectively, are used for the secure transmission of data depicted with the trunk of the tree [67].

There are many architectures proposed for IoT networks, and the diversity of their layers (e.g., monitoring, communication, management, security, etc) lead to appear strengths and weaknesses. For example, table 1.4 represents the limitation of famously proposed architectures at the security issue (on the network, identity management, privacy, trust, and resilience). Adopting these solutions in the smart city threatens information integrity, therefore, these problems should be enhanced by protection mechanisms.

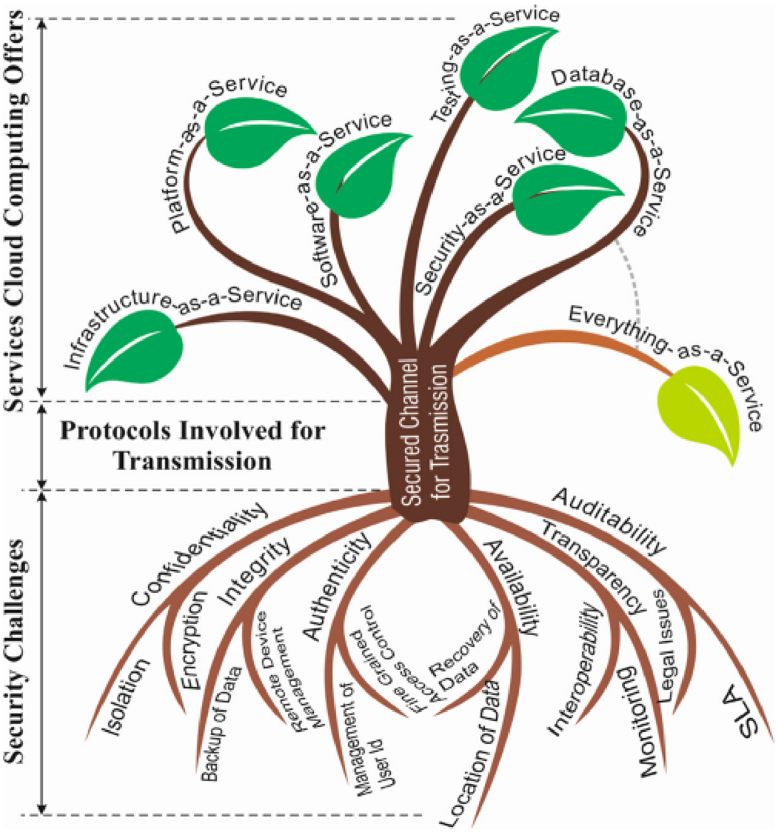


FIGURE 1.3: Security tree [67].

1.4 Objectives

As previously explained, the smart city has several problems. In this work, we will address the issue of protection through blockchain technology. To reach our main aim, we divided the thesis into four secondary goals shown in Figure 1.4. Each goal is addressed with techniques and tools. Tests were applied to confirm the validity of the proposed hypotheses. For each contribution, we provide solutions and obtain results. To show the significance of our work.

1. Giving an overview of the smart city (the spread of the IoT, SC challenges, researchers' trends, SC applications, etc.).

2. Using formal methods, timed automata, sequence diagrams to explain the characteristics of objects, environments, and protocols operations in a smart city.

3. Reducing the cost and maximizing the covered areas on the buildings that connecting the smart components of a smart city.

4. Proposing decentralized solutions to preserve data integrity and manage more efficiently the access control in a smart city information system.

1.5 Thesis Contributions

We summarize the main contributions of this thesis, as follows.

- Representing the behaviors of the building nodes through formal semantics, also, testing their finite-state machines on modeling, validation, and verification tool [69, 70].

- Proposing a hybrid methodology that relies on formal methods and network analysis techniques to ensure the global security and functional requirements for smart cities [71].

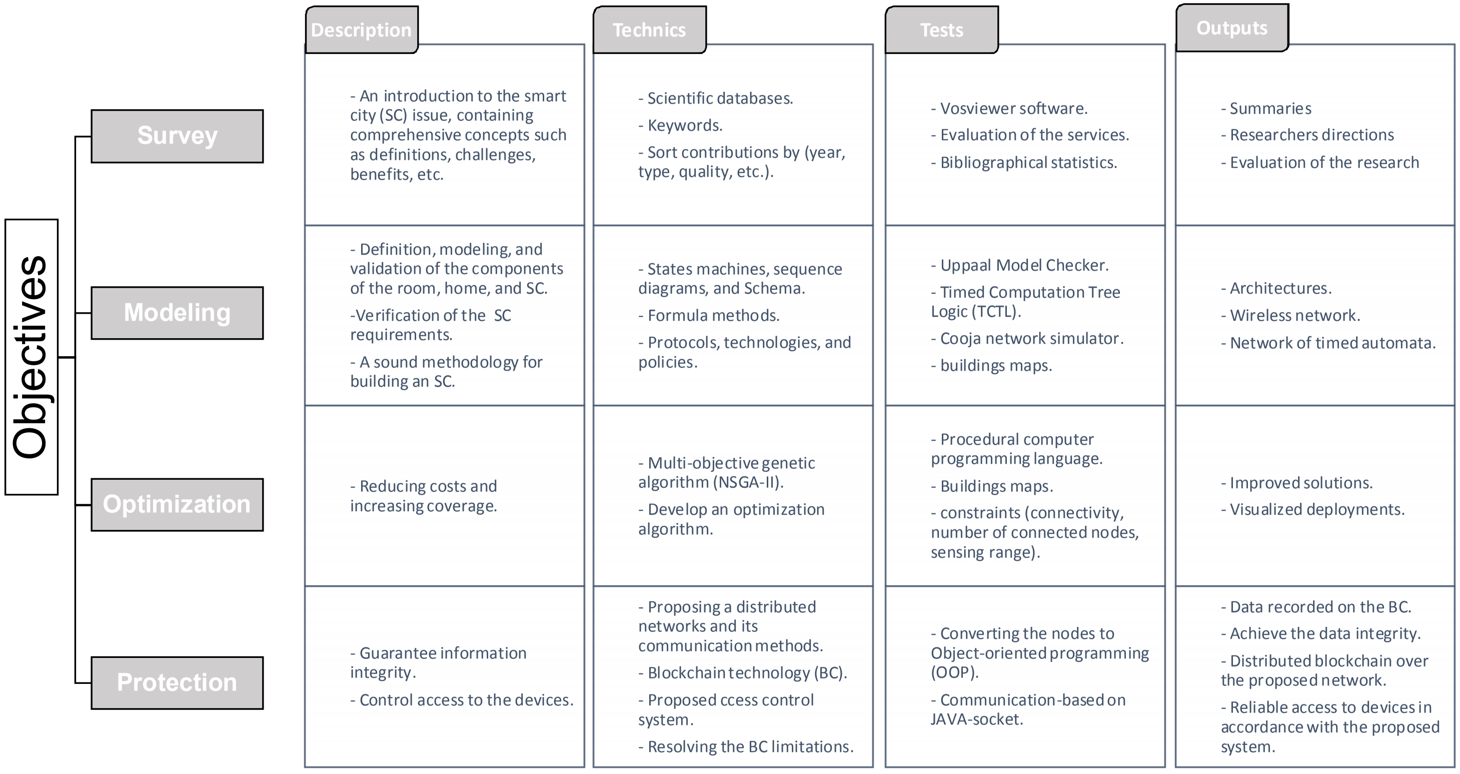
- To maximize the covered areas with a low cost in BIM, automatic deployment of WSNs was presented, the latter focus on the evolutionary algorithm NSGA-II, the improving algorithm, multi-wall model, and obstacles impacts [72].

- Ensure the data integrity in the smart city by developing a system based on the blockchain concept, it consists of heterogeneous nodes, blockchain structure, and organized communication [73].

- Proposing an access control system, it relies on subjects, objects, and tasks, where, their values are protected through blockchain [74].

1.6 Thesis Organization

The thesis is organized as follows.



Objectives	Description	Technics	Tests	Outputs
Survey	- An introduction to the smart city (SC) issue, containing comprehensive concepts such as definitions, challenges, benefits, etc.	- Scientific databases. - Keywords. - Sort contributions by (year, type, quality, etc.).	- Vosviewer software. - Evaluation of the services. - Bibliographical statistics.	- Summaries - Researchers directions - Evaluation of the research
Modeling	- Definition, modeling, and validation of the components of the room, home, and SC. -Verification of the SC requirements. - A sound methodology for building an SC.	- States machines, sequence diagrams, and Schema. - Formula methods. - Protocols, technologies, and policies.	- Uppaal Model Checker. - Timed Computation Tree Logic (TCTL). - Cooja network simulator. - buildings maps.	- Architectures. - Wireless network. - Network of timed automata.
Optimization	- Reducing costs and increasing coverage.	- Multi-objective genetic algorithm (NSGA-II). - Develop an optimization algorithm.	- Procedural computer programming language. - Buildings maps. - constraints (connectivity, number of connected nodes, sensing range).	- Improved solutions. - Visualized deployments.
Protection	- Guarantee information integrity. - Control access to the devices.	- Proposing a distributed networks and its communication methods. - Blockchain technology (BC). - Proposed ccess control system. - Resolving the BC limitations.	- Converting the nodes to Object-oriented programming (OOP). - Communication-based on JAVA-socket.	- Data recorded on the BC. - Achieve the data integrity. - Distributed blockchain over the proposed network. - Reliable access to devices in accordance with the proposed system.

FIGURE 1.4: Objectives of the thesis.

- Chapter 2 explores the background needed for our thesis.
- Chapter 3 develops a robust semantic formalism for smart cities and provides an hybrid approach to build a reliable smart city.
- Chapter 4 shows how to optimally deploy WSNs in the smart city model.
- Chapter 5 demonstrates the integration of blockchain technology into two frameworks that ensure data integrity and access control.
- Chapter 6 concludes our work by summarizing the main contributions in the thesis, and discussing the possible future works that are potential research directions.

Criteria	Traditional City	Smart City	
		Reality	Projects
Energy consumption	• Non-renewable energy [20]. • Energy is polluted [21], where climate change has cost the U.S. economy around 240 billion per year over the last 10 years [22]. • Large number of non-optimized devices. • The characteristics of their protocols do not serve the IoT network.	• Renewable energy [23]. • Small number of IoT devices. • The protocols used by IoT nodes is characterized by a low power as CoAP. RPL, 6LoWPAN, etc [24]. • An electric car emits 22% less CO2 than a diesel [25].	• Photovoltaic power plants construction under the credit program 'Eco-Energy' [26]. • Completely decarbonized power system [27].
Large data	• Collapse of the information system [28], e.g. as happened in Amazon Web Services, the 800-pound gorilla of everything cloud computing [29]. • Low-security level [30]. • Bad service provided.	• Continued operation of the system and smart processing of information [31]. • Very protected system [32]. • Availability and QoS are achieved [33].	• Flexible framework provides dynamic QoS [34]. • Techniques against the distributed denial of service [35].
Coverage and latency	• Small range and low speed of transmitted data due to it uses traditional communication technologies [36]. • Architecture bases to distant servers cause high latency [37].	• Large communication range and low latency due to it uses the high technologies such as 5G [38], theoretically, 5G speed is up to 400 Mbps, while 4G is up to 50 Mbps [39]. • Edge devices connect near stations (Fog computing).	• Maximizing coverage quality with budget-constrained [40].
Buildings	• Difficult to mitigate the building threats like fire, temperature, humidity, etc.	• It has IoT nodes Like sensors that can measure the requirements of building [41], there are many types of sensors, e.g. temperature sensors, humidity sensors, motion sensors, air quality sensors, etc [42].	• Using low-cost sensors to monitor the presence of people in closed buildings [43].
Security	• Information loss due to saturation of the server provider by the data flooding. • More vulnerable system, from many threats like DDOS [44], Black hole [45], and sniffing [46].	• Controlling the user requests. • Modern components with high security.	The enhanced security architecture that covers the new 5G environment [47].
Cost	• Studies have shown that the economic impact of power outages is significant [48]. • Some cities suffer from the cost of recycling waste, e.g. all over Italy [49].	• The city can manage its energy through solar photovoltaic, Thermal collectors, and concentrated solar power [50]. • IoT technologies like RFID, sensors and actuators, and wireless mobile communication technologies can be applied to waste management [51].	• A framework that exploits big data to reduce energy in smart cities [52]. • An architecture based on deep learning and IoT to manage waste [53].

TABLE 1.2: Comparison between smart and traditional cities.

GOVERNANCE	ECONOMY	MOBILITY	ENVIRONMENT	PEOPLE	LIVING
Flexible governance	Unemployment	Sustainable mobility	Energy saving	Unemployment	Affordable housing
Shrinking cities	Shrinking cities	Inclusive mobility	Shrinking cities	Social cohesion	Social cohesion
Territorial cohesion	Economic decline	Multimodal transport system	Holistic approach to environmental and energy issues	Poverty	Health problems
Combination of formal and informal government	Territorial cohesion	Urban ecosystems under pressure	Urban ecosystems under pressure	Ageing population	Emergency management
	Monosectoral economy	Traffic congestion	Climate change effects	S.diversity as source of innovation	Urban sprawl
	Sust. local economies	Non-car mobility	Urban sprawl	Cyber Security	Safety and Security
	Social diversity as source of innovation	ICT infrastructure deficit			Cyber Security
	ICT infrast.deficit				

TABLE 1.3: City challenges in European cities [63].

Requirements	**IoT-A**	**BeTaaS**	**OpenIoT**	**IoT@Work**
Network security				
. . . Confidentiality	✓	✓	✓	✓
. . . Integrity	✓	✓	✓	✗
. . . Authenticity	✓	✓	✓	✓
. . . Availability	✗	✗	✗	≈
Identity management				
. . . Authentication	✓	✓	✓	✓
. . . Authorization	✓	✓	✓	✓
. . . Accountability	✗	✗	✗	✓
. . . Revocation	✓	✗	✗	✓
Privacy				
. . . Data privacy	≈	✗	✗	≈
. . . Anonymity	✗	✗	✗	✓
. . . Pseudonymity	✓	✗	✗	✓
. . . Unlinkability	✓	✗	✗	✗
Trust				
. . . Device trust	✓	✓	✓	✗
. . . Entity trust	✓	✗	✓	✗
. . . Data trust	✗	✓	✗	✗
Resilience				
. . . Robustness	✓	✓	✗	≈
. . . Resilience	✓	✓	✓	≈

TABLE 1.4: IoT architectures and security requirements: "✓" indicates fulfillment, "✗" no fulfillment or missing evidence, and "≈" a partial fulfillment. [68].

Chapter 2

State-of-the-Art: Background, Survey, Comparison, and Evaluation Services

2.1 Introduction

After the information revolution that the world witnessed, many sectors in the city (buildings, health, transportation, etc.) have been digitized with modern devices, so human life has become smooth and safer than before. The smart city is a term resulting from the city's adoption of these technologies, as its systems were characterized by automation and reliability. Efforts are still ongoing, we can know this through the increasing contributions to research databases, the competition of technology companies, and the spread of smart devices among people. Many existing approaches realized the concept of the smart city by developing several aspects including information protection, data management, reducing delays, expanding coverage, etc. These concepts are adopted on all sectors of the city (health, education, transportation, economy, etc.). For this purpose, we survey and classify the most pertinent contributions related to this issue.

The main focus of this chapter are:

1. Surveying the recent contributions discussing key issues of a smart city.

2. Introducing IoT concepts and showing the reason of its spread in smart cities.

3. Identifying the main Keys of developing emergent technologies in the different fields of a smart city.

4. Showing the advantages of a smart city and their impact on individuals and governments.

5. Discussing challenges related to the development of smart cities.

6. Developing an innovative methodology based on measuring requests and responses that can gauge smart city sectors.

7. Using benchmarks to show trends, the dominant concepts, the role and the efficiency of devices in providing best services of smart cities

This section is organized as follows. Section 2.2 is a comprehensive overview of IoT and the smart city. Section 2.3 presents the literature related to the concepts and challenges of smart cities. In addition, our contribution related to the smart city and based on requests/responses of devices has been developed as well as the obtained results are presented in Section 2.4. Finally, we conclude the paper in section 2.5.

2.2 Background

2.2.1 IoT Overview

To define better the Internet of Things, we must detail the two terms separately, then, know how they were collected on one term. The Internet became commercial in the mid-1980s after it was owned by the US Department of Defense only. Where ARPANET (its first name) was divided into two networks, ARPANET was directed to research uses while MILNET was dedicated to military activities to preserve their security [75]. Despite the low services on the traditional architecture (low speed [76], unreliability, low computing/storage [77]) that relies on servers serving computer requests, it has gained increasing popularity due to the saved time, effort, and money.

This demand encouraged researchers, commercial and military institutions to join other devices to the world wide web. These devices were Wireless Sensors Network (WSNs) [78], household appliances [79], GPS systems [80], smart phones [81], etc. These tools were called *things*. So, the idea of the *Internet of Things* was not planned, but rather, it is the result of the information revolution. With a simple definition, the Internet of Things is a huge network of tools and devices that can communicate with each other. Their roles were to improve the users living conditions by adopting the most daily tasks of the users. For example, the sensors distributed in the home can measure the temperature, while the actuators turn on the air conditioner, open windows, and start the car before going, etc. So, the role of the users is to adapt the environment with the devices and then determine the living conditions. Deployed devices have features and behaviors (wireless [82], type of connection, size, cost [83], energy, lifetime, etc) that should conform to the requirements of the environment. Some people believe that the Internet of Things is controlled by large commercial companies, but in reality, it is the result of increased users' requirements, where, the major technology companies spend a lot of money and effort in exchange for obtaining the personal information of users. For example, Adword[1] relies on users' data to market products, focuses on written keywords, and sites owned by Google (such as Gmail, Youtube) [84].

2.2.2 The Spread of IoT

Figure 2.1 shows the number of connected devices from 2015 to 2025, and we note that the number of devices can increase by about 60 billion in just ten years. If we assume that the population of the earth in 2015 is 7 billion people, so, every person will have at least two devices. On other hand, if the number of people in 2025 is about 8 billion, so, each person will have at least 9 devices. The reasons for this huge increase are the following.

- **Development of Information and Communication Technologies (ICTs):** In the last years, both types of communication technologies (wired and wireless) address

[1] it is Google's platform for advertisers, `https://ads.google.com/nav/login`

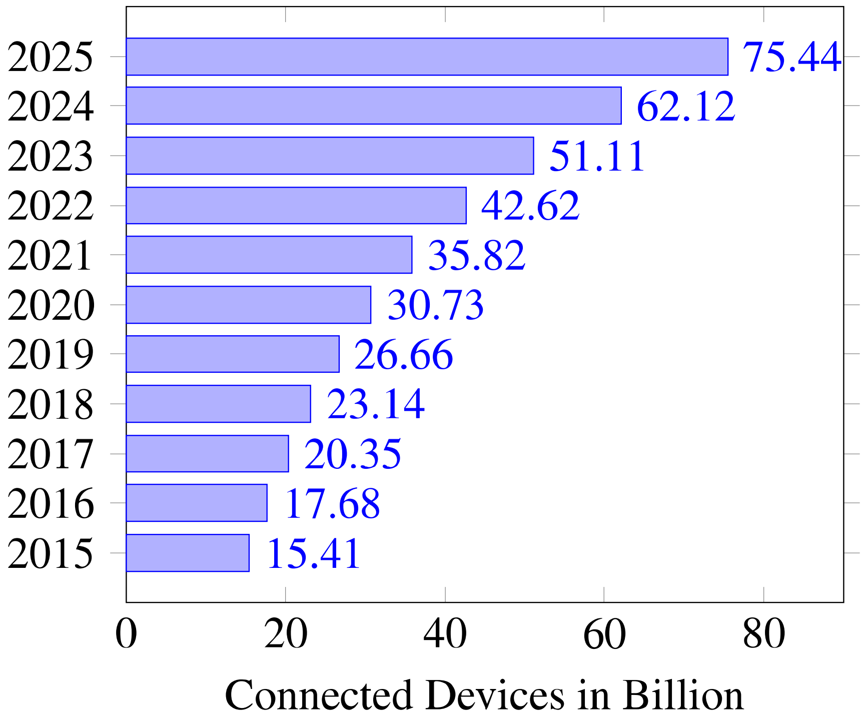


FIGURE 2.1: Number of IoT devices form 2015 to 2025. [85]

the IoT requirements (latency, security, quality, coverage, cost). For example, optical fibers are featured at a high speed among all the wired connections, where, in September 2012, the NTT company announced that optical fiber speed reaches one petabit per second over a distance of 50 Km [86]. According to wireless communications, the last generation of mobile communication (5G) provides a high data flow, which encourages mobile phone users to get it.

- **Competition between companies:** The statistics presented in Figure 2.2 shows that technology companies are dominant in all fields. This leads to an increase in the competition between them, and as a result, devices of high quality and reasonable prices are offered. This consequence is enough to encourage users to acquire additional devices that serve their interests.

- **High risks:** The large increase in the population has caused human and material losses. According to the World Health Organization (WHO), the number of deaths from cardiovascular diseases has reached 17.9 million people in 2019 [87]. Also, the American Fire Administration published in a statement that the number of fires for the year 2019 amounted to 1291,500 fires in the United States [88]. WHO announced that between the years 1998-2017, the tsunami disaster led to the death of 250,000 people in the world [89]. Further, the number of confirmed cases of corona disease on January 07, 2020, exceeded 301685953 confirmed cases [90].

- **Improving the city's sectors:** The recent studies and past events show that the world sees smart devices as the best way to reduce health, environmental, urban, and social problems. This leads to developing systems of fire control [91], pollution control [92], weather monitoring [93], and limiting the spread of the Coronavirus [94].

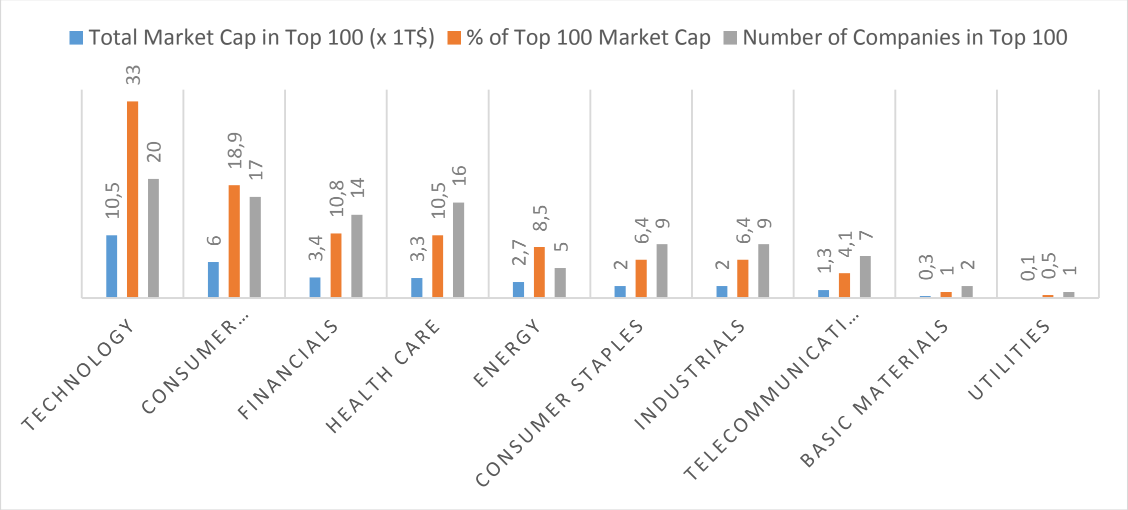


FIGURE 2.2: The 100 dominant companies in the global market [95]

2.2.3 Smart City Overview

The term of "Smart City"consists of two words, where *city* means a wide geographical area that has a high population density, huge infrastructure, and extensive activities in many fields (health, transportation, communication, etc.). This term includes the traditional city, as for the term *smart*, all the parameters, including technical devices, the developed systems, and the management policies [96] are adopted by the city in order to bring many benefits. The linguistic meaning of the smart city is incorrect, as it is not possible for a group of buildings, roads, and transportation to be *smart*, but the smart city' sectors (Figure 2.3) that are smartly managed. In order to upgrade any sector, it is required at least to rely on one of the following four development keys.

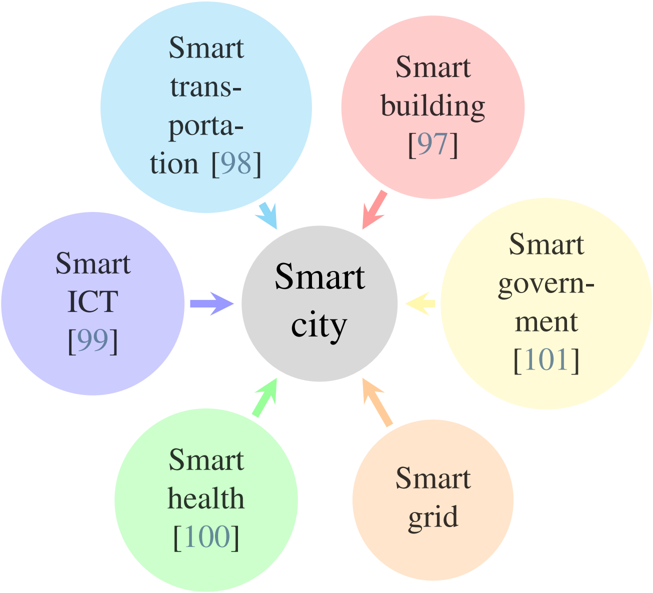


FIGURE 2.3: Smart City Sectors.

1. **The Internet of Things (IoT)** is the best way to link the smart city's parameters to each other due to its given advantages, including low cost, mobility, low latency, real-time monitoring, etc.

2. **Cyber-Physical-Systems (CPS)** is a combination of heterogeneous systems of different aspects (physical, hardware, software, human, and natural) that are enhanced by smart decision supports especially Artificial Intelligence (AI) [102], Machine Learning (ML) [103], and Deep Learning (DL) [104]. CPS create a model capable of performing functions mastered initially by human, like automated driving [105], interactive robots [106], etc.

3. **Modern technologies** offer the abundance and efficiency of modern devices which allow for more information collection, storage, and processing, thus resulting in

few or no errors. In addition to lower costs due to less maintenance, lower energy consumption, and many functions in one device. Also, the services performed from the developed systems satisfy the users' requests.

4. **Management strategies** mean all commands, rules, laws, or policies that control the relationship between users and devices. The user and the device are two variables in one system, where each party is ignorant of the overall characteristics and behaviors of the other party. Strategies are developed to extract the positive points and avoid the weaknesses for each of them. For example, resource access policies [107], the hierarchy of users, security rules [108], etc.

2.2.4 Why the Smart City

Governments should trend through the concept of the smart city, due to the benefits obtained from this advancement. In addition, the traditional problems have changed and multiplied, and smart solutions must be deployed. By comparing the current time to the end of the last century, we note that several problems have emerged that did not exist or were of mild impact, e.g., environmental pollution, traffic accidents, privacy penetration, the difficulty of living, low-quality and expensive equipment, etc. The benefits offered by the smart city are as follows.

- **Low cost:** This is the most important reason the sectors emphasize, as they seek to reduce the users' costs. For example, smart buildings equipped with sensors benefit from outside conditions and exploit them. They can take the advantage of air temperature, daylighting to reduce the cost of electrical energy consumption, or enhancing the home thermostat with a sensing optimization approach [109].

- **Ease and comfort:** City life forces citizens to be busy most of the time. The smart city provides them with the required materials that mitigate or prevent this tired routine. For example, smart transportation that depends on the Internet of Vehicles (IoV) can monitor traffic and give necessary instructions to drivers.

- **Safety:** It is a feature that all sectors give their users, also, it is a primary requirement which we face the city's dangers. For example, smart buildings monitor the status of residents from all internal risks (such as fire and heat) and external (such as earthquakes, rain, wind, etc.), smart healthcare tracks patients remotely and in real-time, ICTs provide their users with physical protection (Firewall, isolated databases, secure phones, etc.) and digital (encryption, protected channels, antivirus, etc). Also, IoT devices can face and reduce COVID-19 disease [110].
- **Quality:** The users are constantly searching for new additions with good qualities, and this motivation inspires the technology forward. For example, the ultra-low-latency of fifth-generation (5G) new radio is very motivating compared to the other communication mobile technologies [111]. On the other hand, several studies have been developed to improve the building system by including all visual, voice, tactile, cognitive, and emotional interactions [112].

2.2.5 Smart City Challenges

First, we refer to the challenges related to each sector of the smart city. Then, we detail the common challenges between them and the most impact ones on the city. In addition, we suggest possible solutions to address them.

- **Density** is generally caused by the huge population compared to the living area. It results in large activities and continuous requests in all sectors. This causes the devices to be unable to treat these demands. The city should be reinforced with the elements required to address this demographic growth [113]. For example, developing a traffic control system based on prediction [114], hybrid charging stations using solar energy [115], etc.
- **Geographical zone** is a large area that requires great efforts to achieve satisfactory coverage through the distribution of contact stations [116]. Negligence in this case leads to the loss of information and thus the lack of a proper

link between sectors and users. On the other hand, a small area causes density, which is difficult to manage, as it requires the government to analyze the places and times of density and then intervene immediately by the necessary solutions.

- **Cost:** The more equipment we have, the more efficient sector is. But, this enhancement costs users a lot of money, which is reflected in the purchase price, energy consumption, and periodic maintenance. Innovations and new generations reduce the cost, for example, the number of nodes using Bluetooth 5 is small compared to the previous technologies (classic and 4.x) due to the coverage range [117]. Also, the use of renewable energies (such as solar energy [118], hydro power [119], geothermal energy [120], wind energy [121], etc.) are successful and necessary. In addition, high-quality objects have a long lifetime [79] which save the maintenance cost.
- **Management of information:** the high flow of information (requests and responses) in the network needs to be managed in terms of protection, storage, processing, routing, and speed. Poor management leads to loss and leakage of information or bad services, while, the ideal management requires to basic mechanisms like: key exchange protocols [122], access control systems [123], super cloud computing, metrics-based routing [124], reduce latency through data replication methods [125], etc.
- **Pollution:** reducing it is the responsibility of all sectors, given that everyone can participate in its occurrence. In addition, its spread causes the waste of human and material energies. It is solved in two ways, the first is to rely on systems using clean energy or using control systems where the weather is monitored and exploited with modern technologies [126].

2.3 Related Work

Due to the climate change and to deal with the sea level rising, Kirimtat et al. [127] suggested an innovative approach named “Smart Floating Cities (SFC)”, that integrated many aspects like smart people, smart economy, smart governance, smart mobility, smart environment, and smart living. They gave the frequent keys to study the most studied issues. Also, they presented the definitions of the smart cities from articles of high impacts They compared the studied literature through the areas of application, proposed methodologies, benefits, and limitations. Finally, they evoked researches with different trends that can be combined with their approach. Although the presented details, the manuscript did not propose a concrete model that shows the relation between the studied contributions. In addition, no methodology is presented to show application of a floating city, ans also, without mentioning the pros and cons of their proposal approach.

Hassan et al. [128] have divided the IoT network of a smart city into three layers: perception, network, and application by highlighting the relation between the computing cloud and IoT. Hierarchically, they have characterized a smart city using features like: mobility, economy, people, living, etc. This categorization was detailed in the context of existing and predefined conditions. Mainly, they explained how the city is exploited in several aspects, namely healthcare, transportation, energy system, and parking system. Further by using the critical analysis, they evaluated the existing works in terms of smart city services, micro-controllers, tools, sensors, network communication, and important results. However, several important points have been tackled but the survey lacked innovation in terms of detailing the concepts and challenges facing smart cities development.

The privacy and security issues within the smart city are primordial to achieve the needed confidence. Ismagilova et al. [129] conducted a survey by searching keywords on Scopus database, selecting the appropriate contribution, and extracting data such as the year, the name of the journal, etc. After that, the found contributions were classified according to the addresses topics, namely privacy and security of mobile devices and services, infrastructure, power system, etc. Several challenges related to the sustainability of the smart city were identified: trust, operational and transition, technological, and sustainability challenges. Moreover, they proposed a framework for privacy and security of the smart city, which combines the smart city challenges and factors.

The evolution of the digital world may degrade the performance of cloud computing, especially in terms of response time, which is one of the most important issues to develop a smart city. Therefore, it is necessary to include fog computing within the city's network. Javadzadeh and Rahmani [130] made an overview of the studies that address fog computing technology in the smart city. Several questions were asked about this issue such as future challenges, how to evaluate the proposed systems, the existing problems and the deployed solutions, etc. The surveyed studies were categorized into the service objective, which means the purpose of exploiting the technology within the smart city (latency, security, mobility, etc.), application classification, which refers to the areas in which this technology can be used (health, energy, education, etc.), and outcome type, which indicates the final results obtained from previous work, such as frameworks. Finally, they did an analysis where they showed the pros and cons of the related works by indicating the addressed service objectives. However, the large number of restrictions when using databases search and keywords specification may reduce research results. We believe this is the reason for not identifying some fields like the smart industry or smart educations.

Data collection can be the mainstay of the automated decisions applied by the devices. So, the correctness of data leads to sound decisions. Ageed et al. [131] studied data mining in the smart city. Initially, they highlighted how big data are depending on mining techniques, the role of cloud computing, and the active components in IoT. They focused on tracking the city's pulse, optimizing data failure services' resilience, standardized Internet, the city's biodiversity, etc. After that, they compared algorithms, tools, and goals with the most important obtained results. Despite recent relevant studied contributions, we notified a lack of data references and benchmarks as well as of visual supports such as charts, curves, tables, etc.

The Internet of Things became a pioneer of smart cities by collecting massive data and executing complex tasks, Smys [132] studied the integration of IoT within smart cities and their. First, the applications of IoT were referred with real examples, including smart living, smart agriculture, smart parking, smart city, smart industry, smart environment, and smart energy. After that, they focused on the challenges faced by this technology such as managing big data, in addition to sensing towards cloud computing, AI algorithms, machine learning techniques. Finally, they detailed each of the concepts with its IoT architecture in smart home, home automation, smart cities. Many examples were presented without criticizing the relevant with a lack of details.

Concretely, the flexibility of a network depends on the smart city architecture. Zhang et al. [133] classified the applications of the smart city on energy, environment, industry, living, and services. Then, they proposed an architecture to control them by modeling: the physical world that contains sensing and operating components, the communication world that integrates the heterogeneous networks, the information world which includes the control, analysis, and stored modules. Finally, they discussed the challenges of security and privacy through some applications by showing the possible mitigation solutions. However, the defined IoT components need more details especially their properties (e.g., the latency, capacities, security, etc). Moreover, the security has been sketched without showing how to deploy protocols within the involved encryption methods. Unfortunately, the experiments have been excluded to validate the proposed approach.

Among the studies made by the deployment of the Wireless Sensors Network (WSNs) in a smart area of interest, Kanaris et al. [134] proposed a methodology to deploy WSNs and IoT nodes in complex urban environments. The aim was to create a preliminary system in network simulators to facilitate the management and deployment of the network in an area of interest. The methodology ran on two steps: the first was to integrate the deployment in TruNET wireless which is a realistic 3D polarimetric physical layer simulator and the second was to export the results obtained from TruNET to the Cooja simulator which is specially designed for WSNs or IoT networks. They concluded that the simulation results did not much the real results, so they were insufficient to build a real network. In addition, the obtained results regarding the physical layer data were less realistic. This problem can be overcome through simulation and verification as well as by covering latency of protocols, propagation signal method, and coverage.

Kacou et al. [135] presented two path loss models for a building map to the objects using the frequencies 800 MHz to 6 GHz. The first model depends on log-distance and the subsequent one is a multi-wall path loss model that integrates the log-distance with the obstacles attenuation. At this end, it is divided into: 1)a generalized multi-wall path loss model that classifies the barriers into two parts dividing walls and load-bearing walls, and the detailed multi-wall path loss model that takes the real values of the obstacles. Kacou et al. [135] focus on the propagation without the sensing operation. Our work deals with the sensing by taking into consideration the distance between the sensor and the target, obstacles impact and the sensing range.

The blockchain technology is used in many domains, for example Raikwar et al. [136] adopted it to achieve the security of the insurance platform, where the transactions processes as smart contract. They implemented the framework on Hyperledger fabric, the results obtained showed that, it is necessary to chose the parameters which constructed the blockchain in order to optimize the network latency. On other hand, the database does not respect the privacy because the data recorded are without encryption. While, Liu et al. [137] proposed a framework of data integrity service, their goal is to create a reliable system that checks the data integrity without third party. Also, Li et al. [138] gave a crowdsourcing system, which receives the tasks from the requester and share them between the workers to solve them, the framework does not consist on third part. The tests show that the system is scalable and applicable.

Nagothu et al. [139] suggested a secure smart service consists on the microservices model and blockchain mechanism, their goal is to make a reliable decentralized system and give a tamper proof of data in the insecure system. The idea is as follows, each microservice records its collected information in its dedicated database. Then, the master database combines these memorizations, after that the miner node extracts its hash which will be added in the new block of the blockchain. They used the smart contract to give the authorized access to the videos captured by the surveillance cameras, the fogs that are near to the edge process in the real time the videos of the cameras, while the cloud computing performs high protection tasks as the reorganization and discovering the malicious intents. The contribution lacks the application and analysis of the obtained results to confirm the effectiveness of the proposed hypothesis. They did not give examples to support the hypothesis, such as object-recognition algorithms, security protocols and hashing mechanisms.

Kushch and Prieto-Castrillo [140] applied the Rolling Blockchain concept to the WSNs deployed in the smart city. The proposed network is considered as distributed servers, where, they contain the blockchain of their sub-clusters and the total blockchain. Since, the WSNs have a low capacity memory, the size of the blockchain depends on the parameters of the "worst" memory node. They gave the mathematical model for the complete chain and the segment of the chain that is removed from the original chain. They constructed a linear distribution of sensors in order to conclude if the network find a new path between two WSNs after the randomly removing of the links. Thus, when they increased the level of attacks (proportion of edges removed), the network always creates an alternative paths until its break down, so the WSN network is scalable. The experiment part did not test the integrity of the data recorded in their proposed blockchain structure. The recording of the blockchain in the WSN makes the network constrained by the worst sensor. The proposed network structure imposes the sensors to apply the blockchain operations (verification, confirmation and storing) that affect the energy storing, the processing and the memorizing capacities which are limited in the sensors.

Jia et al. [141] concerned with increasing the level of protection on the crowd sensing network by the blockchain technique. The network consists of three parts, intelligence crowd sensing networks, confusion mechanisms, and blockchain. The crowd sensing network contains sensors to collect the information users that will be sent to the confusion mechanism. This latter regroups the sensors into 10 nodes, one of them is miner which creates a new block of information. Then, the confusion mechanism integrates the received data in the blockchain, it gives the users virtual coins and puts the encrypted data in the server. After that, the server stores the users' information and motivates the sensor to collect the information. Their contribution encodes the user information using Confusion Mechanism Encode Algorithm (CMA-E) and hashes the blockchain data by Merkle tree algorithm. They created an information storage system through android application that records the data by traditional and CMA-E methods, where a large percentage of people used the second method. However, the complexity of the Merkle tree algorithm is expensive Tn = O(3n). The encoding algorithm is not strong (it can be broken) since it relies on symmetric cryptography techniques.

Cebe et al. [142] create a framework based on the blockchain technology for the forensics of the accident vehicles, it is composed of a forensic daemon inside the vehicle which receives the information from the Event Data Recorders (EDR) and broadcasts Basic Safety Messages (BSM). The forensic daemon publishes the EDR and BSM to the insurance company and the car manufacturers, these latter collect those data to analysis its. The framework does not focus on the types of wireless communication technologies that require high data transmission speed and protection.

Paillisse et al. [143] achieved an access control framework through LISP control plane and the blockchain implementation (Hyperledger Fabric [2]). Its architecture based on three layers, the first layer is the policies defined by the administrator, that grants the users to access the resources, the second layer is the blockchain which stores all users, companies, and policies; and the third layer is the network which is a set of users, resources, protocols that achieve the access operations (requests-responses). The idea was tested on experiment and verified in terms of scalability and network latency. On the other hand, its contribution does not concentrate or lack of validation users, also, the structure of block is very basic.

Islam and Madria [144] enhanced the IoT system by a permissioned blockchain which is consisted on the access control model. The latter is implemented in Hyperledger Fabric which is called Attribute Based Access Control (ABAC). Its proposition collects all of : 1) Actors which are the resource provider and the requester, 2) Components that are a local IoT network and the blockchain , and 3) Resource access process by the requester.

[2] an open-source implementation of a permissioned blockchain

With the tested system, they adjusted the values which serve its experiment. The result showed that, the access request of its access control system is faster compared to the public blockchain. On the other hand, the latency increases by increasing the number of attributes in the policy.

The goal of Novo [145] is to propose a decentralized access control system for the IoT devices by using the blockchain technology. The system is composed of WSNs, Managers are responsible for the access control permissions, Agent node deploys the smart contract, smart contract contains all the operations allowed in the access management system. The blockchain network which can be readable from all but only written by the private nodes and Management Hubs that are interfaces which translate the CoAP message received from IoT devices. He evaluated the overall delay of the architecture when including the management hub nodes. The performance of the IoT device is acceptable, but the solution had a waiting issue of the blockchain network to release access control information.

However, achieving a safe and well-built smart city requires continuous maintainability and improved approaches. Thus, any recommended methodology must determine the effective and optimal solutions through the following steps.

- Classifying the application areas, as in Figure 2.4, that need more deep research (e.g., medical informatics, multimedia technologies, computer network and communication, etc).

- Identifying the strengths and the weaknesses of of each selected initiative.

- Determining the reliability degree.

- Standardizing and unifying the solutions in a synergy platform.

- Guaranteeing the inter-operability between all services and deployed solutions.

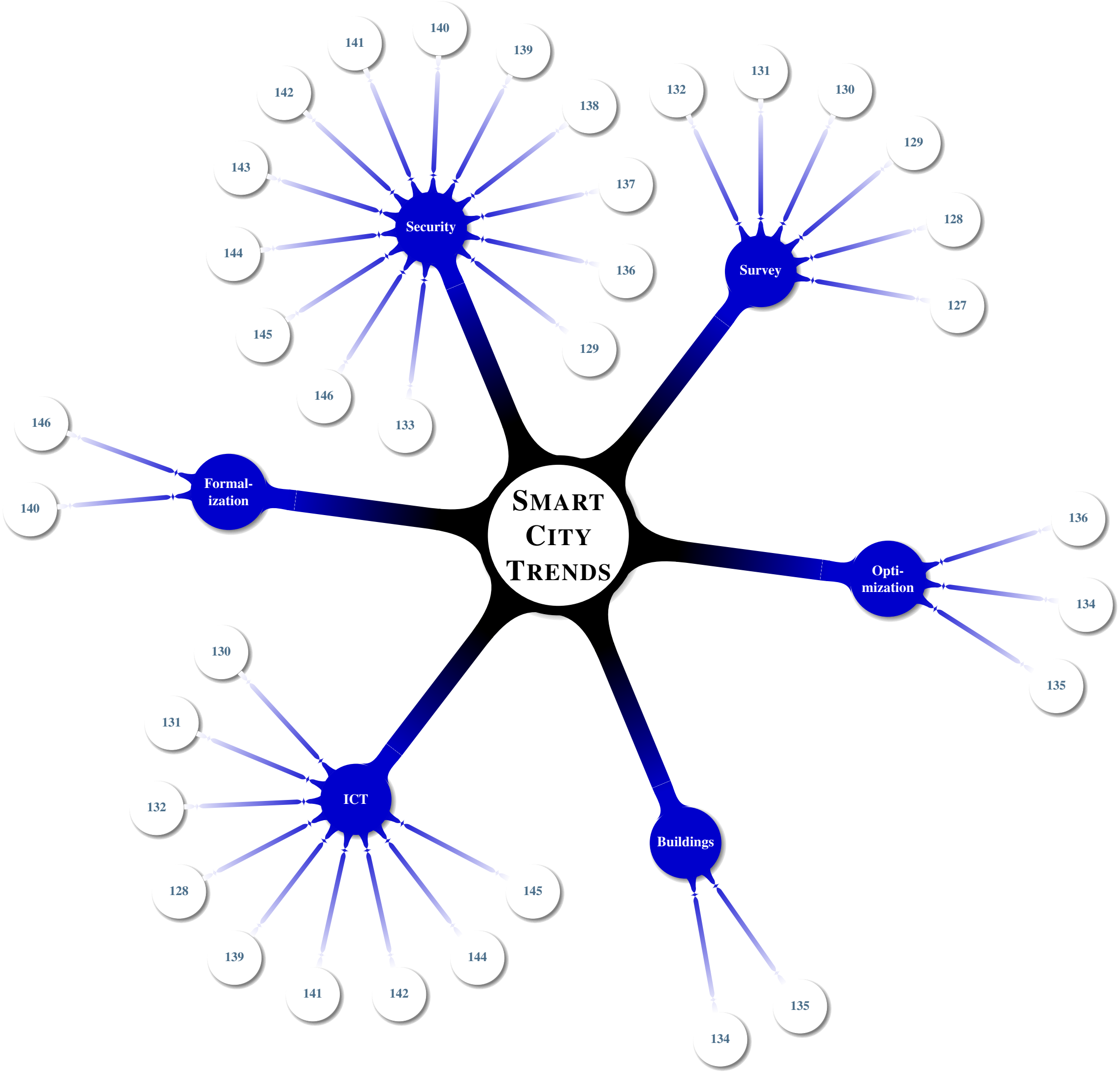


FIGURE 2.4: Smart City Research Applications.

2.4 Evaluating the Services Reliability in Smart Cities

In this section, firstly, we detail our approach about how the sector handles the received requests and then replies them with a sequence of responses. Secondly, we gauge how well a sector is successful. Then, this evaluation guides us to innovate and deploy solutions for unsatisfactory services. Figure 2.5 shows that the sector consists of IoT devices and others constituting interconnected systems (e.g., healthcare [147], education [148], transportation [149]). At any time, sectors are ready to receive an unlimited number of requests. The source of requests may be the users of services (citizens, workers, customers, etc.), and devices where their configuration allow detecting a specific sector to send the appropriate requests. So, automated orders are issued under specific conditions. For example, sudden heart attacks can be monitored by a sensor connected to the patient. In the case of a heart attack, the sensor informs the appropriate doctor of the necessary information (such as the patient's name, room number, previous diagnoses), so, the patient will get the care in real-time.

To avoid any saturation or our of services, we point out that each device (cloud, fog, Bridge, Gateway, etc) has a threshold for receiving requests and considering reliability is fundamental to ensure the resiliency of the global system and inter-operable services. Also, the compatibility of the device within the network is a sensitive matter that must be studied before a saturation occurs. For example, it is not possible to connect a receiving server of limit capacities with very active transmission points. In the normal case, the target devices, satisfy the requester' demands through responses which can be reading/writing information or applying actions.

The smart city is being developed from several directions, where, researchers focus more on specific aspects. For this purpose, we exploited Scopus' database [3], highlighting the contributions related to the smart city in 2019,where we targeted many areas of interest: computer science, engineering, social sciences, and energy. The result showed in Figure 2.6 and they are obtained by using VOS Viewer software [4]. The visualization represents all the index' keywords repeated more than four times, and we ignore similar words (such as IoT and Internet of Things) where we give priority to the predominant term. Keywords are divided into 7 clusters of different colors, the size of the circle indicates the weight of the keyword, while the link between two items mean the existence of a relationship between them. We conclude that researchers are developing a smart city with a close focus on the Internet of things, energy efficiency, energy utilization, security,

[3] https://www.scopus.com/

[4] https://www.vosviewer.com/

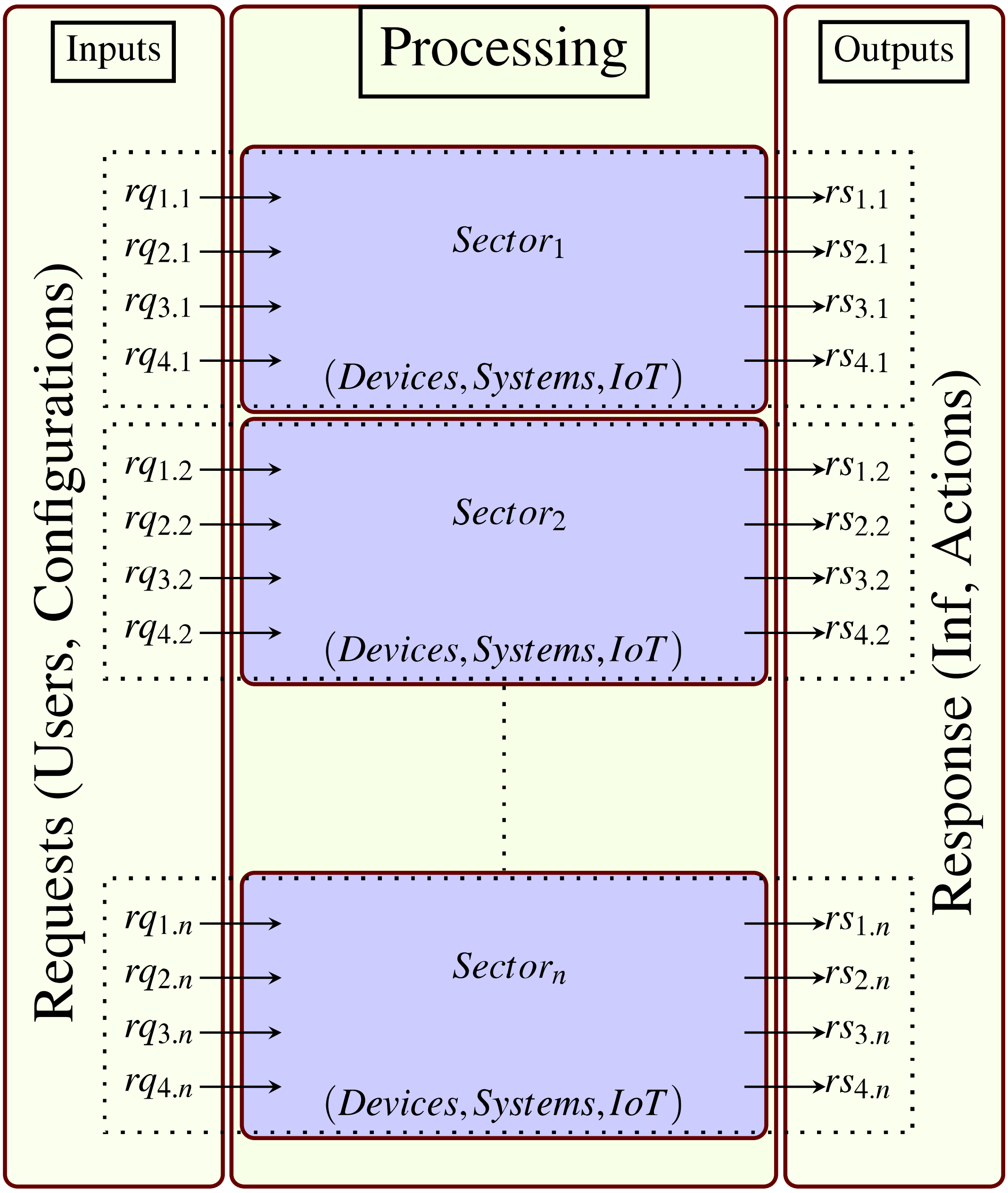


FIGURE 2.5: Data-flow (Requests & Responses) Applied in Smart City.

automation, urban planning, big data, etc.

Based on the previous results, we wanted to examine the research on the most frequently used keywords (internet of things, energy utilization, security , automation, and big data) between 2010 and 2020 in the same database. The obtained results, shown in Figure 2.7, demonstrate that there is a great focus on those keywords and they have a

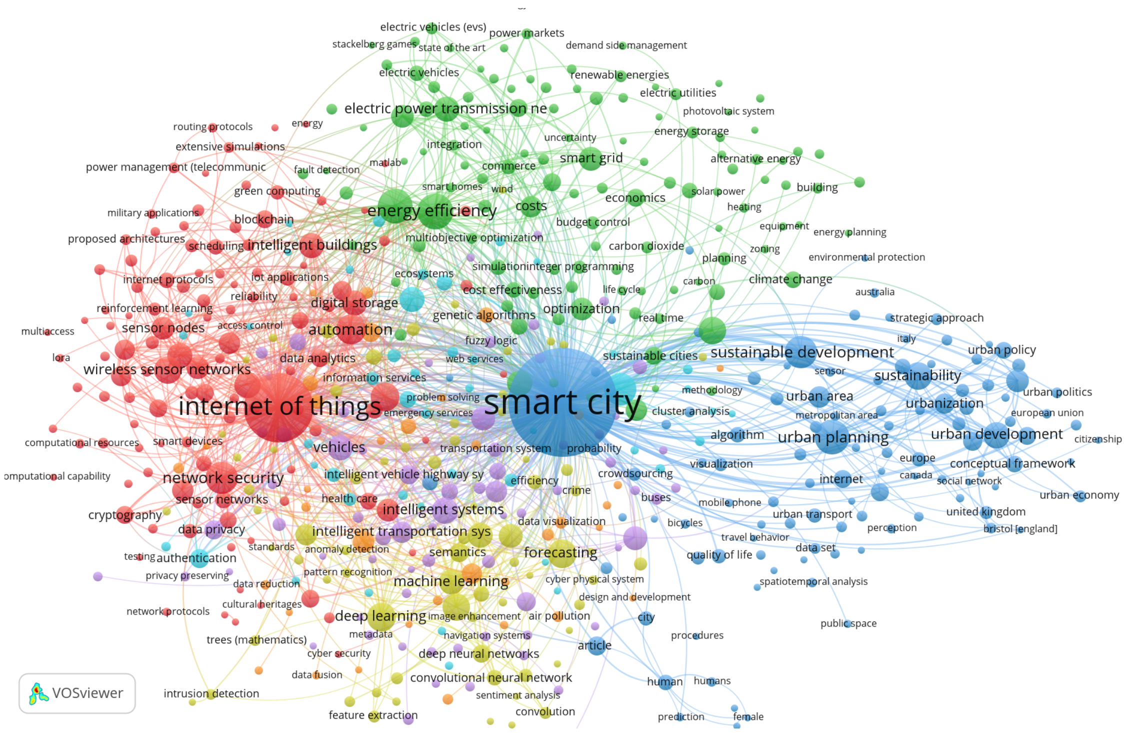


FIGURE 2.6: Building bibliometric networks of researches related to the smart city.

major impact in making the smart city a reality.

The goal of the experiment is to show the effect of the devices' features on the quality of service, and this encourages to configure the network with devices of high capacities. that guarantee the continuity of the system. Using Java programming language, we created ten devices (objects), which receive the requests, then run for a random time between [0.2, 2] seconds. A thousand requests (piratically are the calls) were randomly sent to the devices, the delay time between each request is between [0.001-0.1] second. Devices receive limited requests (which signify the memory), and they ignore requests when they are saturated. Figure 2.8(a) shows the effect of memory on the occurrence or absence of the service, where, the higher the memory capacity, the higher is the response. The test emphasizes this idea, satisfactory service depends on the quality of the materials' features.

On the other hand, Figure 2.8(b) shows the satisfaction ratio of one sector, calculated by Algorithm 1. This process enables us to identify the quality of a services (low satisfaction rate), which helps detect its weaknesses and then improve them.

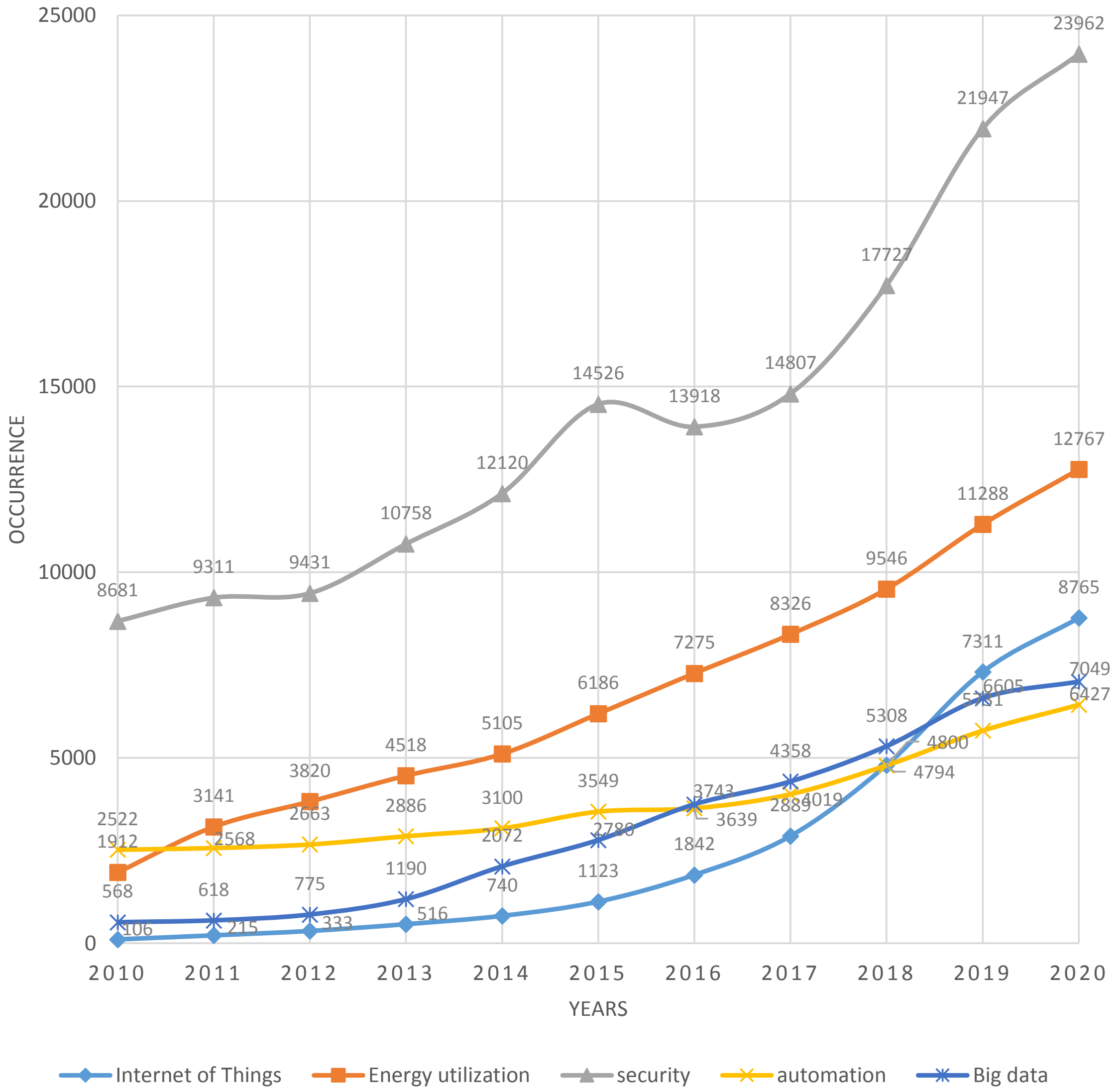
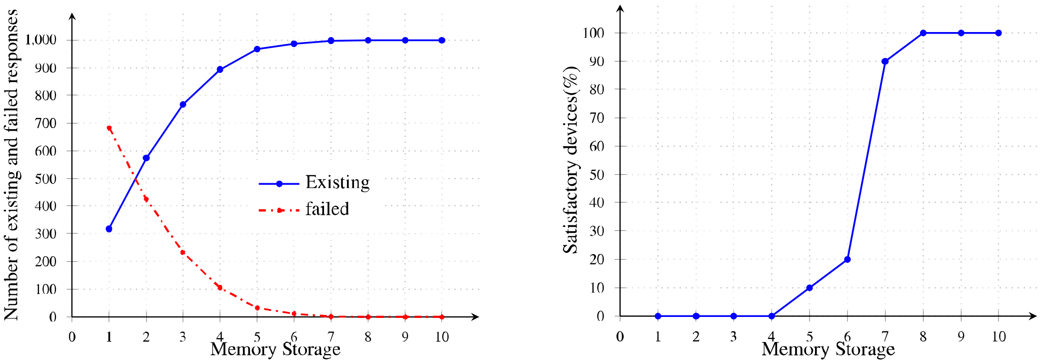


FIGURE 2.7: The occurrence of concepts in scientific articles between 2010 and 2020.

2.5 Conclusion

In this chapter, we have defined the IoT concept and its expansion in the smart city, and also we have introduced the most important services that migh found in a smart city. In addition, we developed a methodology for assessing successful and unsuccessful sectors. Furthermore, through scientific databases, we have shown the trend of hot topics related to smart cities and the most exploited directions. In the next chapter, we will model the most effective nodes in smart rooms, homes, buildings, and smart cities. This part is important



(a) The number of responses in terms of memory size.

(b) The percentage of satisfactory devices in terms of memory size.

FIGURE 2.8: Statistics of responses and satisfaction in terms of devices memory.

Algorithm 1: Calculation of the Satisfactory Sectors

```
for $j = 1$ to $J$ do
                                            // J: The number of all sectors.
    for $i = 1$ to $I$ do
                                            // I: The number of sector' devices.
        if $Response(Device_{ij})/Request(Device_{ij}) \geq 1$ then
            // $Response(Device_{ij})$: returns the number of replies answered by the $Device_{ij}$.
            // $Request(Device_{ij})$: returns the number of requests demanded to the $Device_{ij}$.
            Satis_Sect ++        // $Satis\_Sect$: calculates the number of satisfactory devices on the sector.
        end
    end
    $Rate\_Satis\_Sect_j = (Satis\_Sect \times 100)/I$    // $Rate\_Satis\_Sect_j$: calculates the percentage of satisfaction in all sectors.
end
```

for describing the global model of a smart city. Further, we will suggest a hybrid approach that merges both formal methods and network analysis techniques to enhance the building of a more robust and reliable smart city.

Chapter 3

Sound Formalism and Robust Analysis of Smart Cities

3.1 Introduction

As we explained previously, the smart city is a concept treated by the researchers and the stockholders, also, each integrated field is equipped with specific materials and objects. The smart building plays a sensitive role in the city, due to it is considered a comfortable place for the inhabitants and protects the integrated tools from external threats (like temperature, humidity, crimes, etc.). Many Models (like UML, State machines, SysML, etc), languages (like natural language, formal methods, object-oriented programming, etc), and analyses (like network simulators, dashboards, spreadsheets, etc) are used to study the interactive actions applying between the components in the whole system and analyze the results (i.e. errors or correctness). Formal methods are one of the best ways to represent the behaviors of objects due to it is based on mathematical logic, this stage is verifiable for troubleshooting. On the other hand, the Uppaal model checker is a validation and verification tool that collects the timed automata of objects and tests the best functioning of the global system. In addition, IoT equipment can be simulated in the analysis network like Cooja which shows the collected data and the routing processes in the designed environment.

In this chapter, we will treat the smart building issue in the smart city through all the following steps, Firstly in section 3.2, we review the related works of IoT, building requirements, and smart city applications. In section 3.3, we will propose a smart living framework for smart rooms by modeling the different components needed for an indoor environment and developing a trustworthy architecture. Then in section 3.5, we propose a smart living framework for smart buildings, where, we rely on the existing limitations and the requirements for a home, the proposed solutions consider all indoor issues, implement sensors for each measure, collect data in real-time and make reactions to prevent risks. Also, in section 3.7, we represent our smart city model which combines the physical and the digital models and details our methodology that analyzes **SCM** by ensuring its correctness and security. At the end of the chapter, a conclusion 3.9 is given that concluded this contribution.

3.2 Related Work

In this section, we will review the existing work related to IoT modeling, functional analysis, network architectures, and application in real life with concrete cases.

Firstly, Ouchani *et al.* [146] proposes a security analysis framework for IoT that covers the probability and costs of actions, formalizes IoT, analyzes the correctness and measures their security level by relying on the probabilistic model checking PRISM. To ensure the functional correctness of an IoT-based system, Ouchani develops five steps: defines the IoT components, formalizes the architecture in a process algebra expression. Then, it expresses the IoT requirements in PCTL and transforms the IoT model into the PRISM input language. Finally, PRISM checks how much a requirement is ensured on the IoT model. However, the proposed framework involves a large amount of data and messages which make the probabilistic model checking expensive in terms of time and memory.

Also, Moreno-Salinas *et al.* [150] proposes a method that detects the optimal position of sensors to receive information from several targets. To find the perfect place, they rely on FIM[1] to measure the amount of information that a random variable (sensor) carries about a parameter that is sometimes unknown (target). After several progressive tests, they use two separated tests, the first tries to find the optimal position for a sensors that receives from a target transmitter with a known placement. The second one finds the optimal positions of sensors with unknowns positions. However, FIM showed significant results for a small amount of objects but the cost of calculation time is expensive when the target is unknown in a known area.

Moreover, Al-Fuqaha *et al.* [151] suggest to make IoT protocols compatible with each other by creating re-programmable gateways through a rule-based language. Mainly, they focused on healthcare applications, a nursing home patient monitoring system, a system for the monitoring and mitigation of eating disorders, and an indoor navigation system for the blind and visually impaired people. For the first application, they collect patient measurements in multiple nursing stations by the IoT protocols. In the second application, the patient has a glove that gathers information about the movement of his hand and sends it to a gateway, which translates these messages to deliver the required functionality. The third application uses real-time location services (RTLS) for blind and visually impaired people who run this service and to provide users with tactile navigation information to help them avoid obstacles. In fact, programmers can improve the gateway rules, but it is hard to write in general.

Furthermore A. Zanella *et al.* [152] apply the principles of smart citys for Padova city to collect environmental data. The architecture is composed of constrained IoT sensors, a database server which use technologies CoAP[2], 6LoWPAN[3], unconstrained devices that use traditional technologies like HTML. The interconnection between users and sensors is made by an intermediary gateway and HTTP-CoAP proxy-grown that plays the role of translator between the two sides. During a week of tests, the results show how do people react with different situations and phenomena, for example benzene consumption at the end of weeks. This architecture allows the compatibility between constrained and

[1] Fisher information matrix

[2] Constrained Application Protocol

[3] IPv6 Low power Wireless Personal Area Networks

unconstrained devices by a cross proxy. In general, the constrained physical and link layer technologies are characterized by a low energy consumption, the transfer rate and data processing in constrained devices is relatively low, but the dependence on unconstrained ones increase in cost.

Several research initiatives have been proposed for the smart city with a focus on IoT modeling, smart city components and requirements, and others on indoor management. This section surveys the recent literature related to them.

The term smart city includes many aspects, this is what Saraju .P *et al.* [153] touched upon, where, they presented general definitions about the smart city. They covered them as generalities in terms of applications (smart infrastructure, smart transportation, smart energy, smart healthcare, and smart technology), requirements (sustainability, quality of life, urbanization and smartness), impacts (society, economy, environment, and governance), and infrastructures (physical objects, ICT, and the service). This contribution is rich in concepts but it needs more experiments to demonstrate how the mentioned applications function together.

Further, Centenaro *et al.* [154] focused on the wireless telecommunication LPWANs[4] in a smart city using *LoRa*$^{\text{TM}}$. The aim was to estimate the number of nodes to cover a smart city (inexpensive or not) and to show their advantages after the deployment. They experimented *LoRa*$^{\text{TM}}$ on 19 floors of a building to measure temperature and humidity through one gateway and 32 nodes. Then, they estimated the number of the needed gateways to cover Padova city. They deployed a gateway without antenna gain in a building of two floors to assess the 'worst case'. The obtained result showed that *LoRa*$^{\text{TM}}$ technology could cover a cell of a 2 km radius. They also concluded that 30 gateways were needed to cover Padova. However, *LoRa*$^{\text{TM}}$ had an acceptable range of coverage in worst cases, but the number of ports of the gateways was limited and did not support the evolution of IoT technology.

Concretely, the flexibility of a network depends on the smart city architecture. K.

[4] LowPower Wide Area Networks

Zhang *et al.* [133] classified the applications of the smart city on energy, environment, industry, living, and services. Then, they proposed an architecture to control them by modeling: the physical world that contains sensing and operating components, the communication world that integrates the heterogeneous networks, the information world which includes the control, analysis, and stored modules. Finally, they discussed the challenges of security and privacy through some applications by showing the possible mitigation solutions. However, the defined IoT components need more details especially their properties (e.g., the latency, capacities, security, etc). Moreover, the security has been sketched without showing how to deploy protocols within the involved encryption methods. Unfortunately, the experiments have been excluded to validate the proposed approach.

Practically, the real-world application is the best way to study the behavior of the appliances. Luis Sanchez *et al.* [155] proposed an architecture to monitor the air quality, luminosity, noise, temperature, irrigation monitoring and environmental station in Santander city (Spain). The architecture was composed of three levels: IoT peripherals such as the sensors and APIs, the gateway level, and the IoT server located in the cloud computing service. They tested the architecture to monitor the temperature and the humidity of soil by giving the users access control to their resources through OTAP technology since the solution was not wired. Compared to our contribution, it needs to include the control of sensors and the used protocols to estimate the protection level, and the transmission cost and coverage.

Additionally, among the studies made by the deployment of the Wireless Sensors Network (WSNs) in a smart area of interest, K. Loizos *et al.* [134] proposed a methodology to deploy WSNs and IoT nodes in complex urban environments. The aim was to create a preliminary system in network simulators to facilitate the management and deployment of the network in an area of interest. The methodology ran on two steps: the first was to integrate the deployment in TruNET wireless which is a realistic 3D polarimetric physical layer simulator and the second was to export the results obtained from TruNET to the Cooja simulator which is specially designed for WSNs or IoT networks. They concluded that the simulation results did not much the real results, so they were insufficient to build a real network. In addition, the obtained results regarding the physical layer data were less realistic. This problem can be overcome through simulation and verification as well as by covering latency of protocols, propagation signal method, and coverage.

Also, Hemant . G *et al.* [156] proposed an approach for smart homes and buildings to monitor the life of inhabitants by detecting the inhabitant's events that were collected from IoT nodes (sensor, coordinator, and the gateway). Also, they discussed the mitigation that can be deployed for the connectivity of the IoT system by taking into account the physical separators. However, the proposed architecture did not deal with the integrity of the measured data, and it required an action level to execute the operations according to the collected data.

Furthermore, to improve the level of protection of the Constrained Application Protocol (CoAP) and the encryption in DTLS protocol, S. Arvind *et al.* [157] set a client/server architecture, which was composed of the constrained devices that communicate together through CoAP protocol. The establishment of the architecture has been done by the Cooja simulator installed in the Contiki OS. They intercepted the communication by installing a proxy system in the middle to simulate the sniffing attack. As a result, the data was transmitted in plain text which increased the possibility of attacks on CoAP. Since the DTLS protocol used strong encryption, it is difficult to evaluate its security level by simulation. In addition, this type of attack needs powerful resources to be broken.

Concerning the reviewed initiatives in solving problems related to the smart city and IoT applications. Our focus is to compare our contribution within the literature in terms of **automation** (automatic analysis of **SCM**), **security** (respecting the security requirements), **architecture** (scalable and supporting different ranges of components), **access control** (manage the access authorization to **SCM** resources and components), and **analysis** (the used technique to check and validate the smart city requirements). We found that our contribution covers the identified issues compared to the reviewed ones.

we sought to make a comparison between them shown in Table 3.1, to clarify the points that we touched on, which are automation (automatic analysis of **SCM**), security (respecting the security requirements: confidentiality, data integrity, and the availability

Contribution	Automation	Security	Architecture	Access Control	Analysis
[146]	✓	✓	×	×	✓
[154]	×	×	✓	×	✓
[133]	×	✓	✓	✓	×
[155]	×	✓	✓	✓	✓
[152]	×	✓	✓	×	✓
[134]	×	×	×	×	✓
[156]	×	✓	✓	×	✓
[157]	×	✓	✓	✓	✓
Our contribution	✓	✓	✓	✓	✓

TABLE 3.1: Comparing our contribution with the reviewed initiatives.

of services), architecture (rich and scalable architecture composed of digital and physical components), access control (provide the access authorisation to **SCM** resources and components), and analysis (simulation checks and validates the smart city requirements).

3.3 Smart Room Case

For a better living quality, the smart spaces paradigm aims at constructing advanced service infrastructures that follow the ubiquitous computing approaches where smart objects are executed on a variety of digital devices and services are constructed as an interaction of agents in a communication environment [158]. The main feature of this technology is the integration of heterogeneous and action elements (actuators) in a distributed system that performs different actions based on the information gathered by the sensors combined with the requirements of the particular application. Intelligent information systems enable the processing of multimodal data collected by the sensors, so as to reconcile heterogeneous information and safe conclusions on the facts giving rise to the activation of the necessary actions to address the consequences of these events [159].

The room has several factors that can affect it or the life of inhabitants or both at the same time (temperature, humidity, noise, light, *etc*). Nowadays different numerical models are available to describe the vapor balance of transient water in a room and predict indoor humidity [160]. In general, sensors communicate directly with the home gateway and feed the system information with regards to the obtained environment measures, for example light intensity inside a particular room, temperature inside and outside the home and motion sensing to name a few [161].

In this chapter, we propose a smart living framework by modeling the different components needed for an indoor environment and developing a trustworthy architecture that ensure the well functioning correctness of such system, and also its configuration and control. First, we rely on the existing limitations and the requirements for a room that can affect the inhabitant like humidity, the temperature, loud noise, the challenges of handicapped, dangerous natural and artificial phenomena such as earthquake and fire.

The proposed framework is a web service based solution where sensitive nodes are indoor planted and their measures change in real time. The architecture proposed for the framework considers different classes of nodes. A database node containing the collected data by sensors, a server node that ensures the communication and the reliability between nodes, and reacts when necessary by sending the appropriate control commands; the actuator node executes the received commands from server (actuator) and external actors who can extract or edit room data. The architecture uses MQTT protocol [162] to ensure a reliable communication between the the predefined internal nodes. Further, the architecture implements a precise constraints and requirements for the communication and during executing actions. Otherwise, the nodes do not respecting certain conditions are considered as Unacceptable nodes. Finally we ensure the functional correctness of the nodes and their safe communication by simulation in, the verification and validation tool, Uppaal [163] by creating different scenarios. The results show that the proposed framework is a deadlock free and respecting the indoor living requirements.

This section details the proposed secure network and communication system for smart rooms. First, we present the overall system architecture and the components related to the system, then we detail the semantic of each used object and node, Finally we describe the communication protocol and the data management in the proposed system.

3.3.1 Architecture

Figure 3.1 depicts the main components of the proposed architecture, which is based on three levels, detection, analysis, and action level. The detection level allows to sense the status of a room in real time then it makes a declaration in case a contradictory status (fire, noise, humidity, etc.), the nodes of this level are mainly the sensors. The analysis level has nodes that import the data(input data) to analyze them then extract the commands(output data). Nodes of this level can be either: web server, broker, database, and smartphone. The action level contains actuators that execute the physical actions according to the received commands form analysis level.

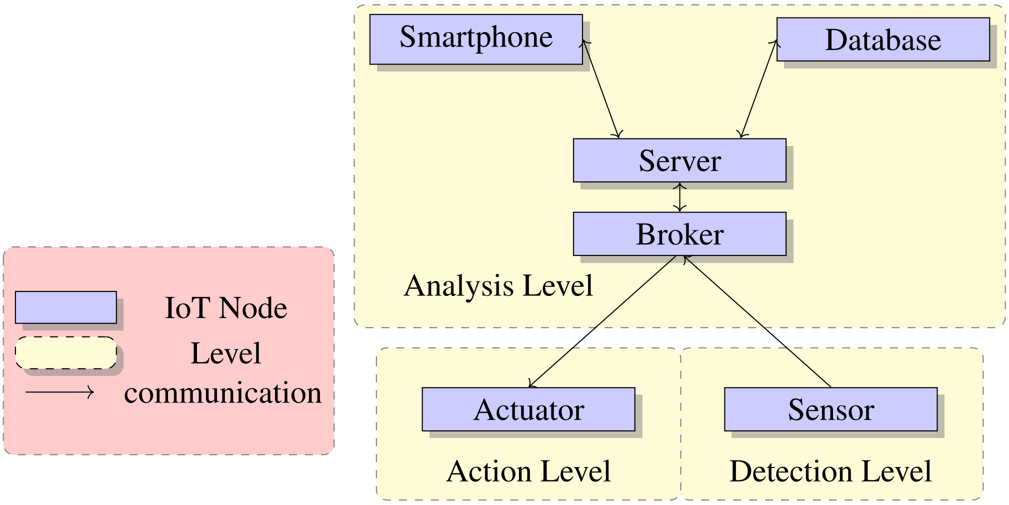


FIGURE 3.1: Architecture of Smart Room.

3.3.2 Smart objects

An object can be defined by its static attributes and dynamic behavior. The static attributes can be: identification [164], connectivity [165], battery life[166], powered by electricity, data security [167], small size, high product quality, constrained device [168], price[169], service availability [170], minimum error[171], easy to maintain, required a low connection rate [172], interoperability of nodes[173]. The dynamic defines its behavior that relies on its proper actions, mainly: turn on[174], turn off[174], send[175], receive [175], collect data [175], apply action[175], encrypt, decrypt, and authenticate. Definition 3.3.2 defines formally a general smart node can be a Sensor, Actuator, Broker, Database, Server or Smartphone.

[Smart node]

A smart node is a tuple of$\langle O, Prop_o, Fonc_o, Behav_o \rangle$, where:

1. O is a finite set of IoT objects written in the form $\{O_i \mid \text{i} \in \text{N} \}$ where $o_\varnothing \in O$ is an empty object.

2. $Prop_o$: O: $\rightarrow 2^A$ is a function returning an object properties where A={Id, Co,BLi , PEl, DSe, SSi, HPr, CDe, LPr, SAv, MEr, EMa, RLo, INo} that precise respectively: identification, connectivity, battery life, powered by electricity, data security, small size , high product quality, constrained device, low price, service availability all the time, minimum error, easy to maintain, required a low connection rate, interoperability of nodes

3. $Fonc_o$ are the set of functionalities/actions of objects, where $fonc_o$ ={ $turn\_on_o$, $turn\_off_o$, $send_o$ (O_i,O_j), $receive_o$(O_i,O_j), $collect\_data_o$, $apply\_action_o$, $consume$ $\_energy_o$,$encrypt_o$, $decrypt_o$, $authenticate_o$ (O_i,O_j) où O_i,$O_j \in$ O }. $turn\_on_o$ and $turn\_off_o$ to turn on or turn off the object, $send_o$ (O_i,O_j) et $receive_o$(O_i,O_j) to send or receive the information from O_i to O_j, $collect\_data_o$ to collect the received information , $apply\_action_o$ to apply an action after getting command, $consume\_energy_o$ the ability to raise the energy level, $encypt_o$ and $decrypt_o$ encypt or decrypt the message, $authenticate_o$ (O_i,O_j) the object O_i authenticate in the object O_j.

4. $Behav_o$: O $\rightarrow E_o$ returns the expression E_o that defines the behavior of an object in the dominant case; where : E_o =$Start.Action.End$; where $Action = Fonc_i|Fonc_i.Action$, $i \in N$

3.3.3 Measurements

We describe here a selection of natural measurements from others that we took into consideration.

- Light: if the noise level measured by the noise sensor in the room reaches a high limit and the room has a low light level as at night, the lights automatically turn on, this case solves the problem of crying the children in the room. In another case, if an inhabitant wants to light a room, the sensor of the light placed on the outer face of the window senses the degree of the sunlight, and if it is enough, the windows will be opened with a turn off of the lamps. This action helps in saving energy.

- intelligent doors and windows: persons with reduced mobility that move by a trolley find it difficult to open the door, so a detector is placed on the door in order to detect the patient trolley . Also other vibration sensors are placed on the wall to detect the earthquake, and if the level is strong, the actuators receive commands that allow the opening of doors and windows to facilitate the exit and to decrease the pressure which can cause a burst of glass, and the another actuators cut the electricity.

- Temperature: to control the energy, the room must contain two temperature sensors, indoor and outdoor. If the temperature service in the server receives the air information from the sensors, the server sends a command to the air conditioner to adjust the temperature level or turn off.
- Humidity: the humidity sensors are placed on the room walls and periodically they measure the level of humidity. If it exceeds the required limit, the sensors declare the humidity service which informs the resident by email for this case, then it gives orders to the actuators to open the windows of the room, and turn on a fan for air circulation in the room.
- Fire: fire sensors trigger automatically the case of fire by measuring the proportion of smoke, and it sends a signal to the fire service in the server, which send commands to the actuator to open doors and windows, spraying water, and the owner of the house and firefighters receive an alert message.

3.3.4 Communication Protocols

The communication between client-server nodes is based on two protocols: MQTT and HTTP. The former, a publish-subscribe mail protocol, is used when sensors and actuators are clients; and the latter is applied for other clients like smartphones which is based on Internet. Figure 3.2 shows the whole communication between nodes, where the main steps are described as follows.

1. A sensor *publish* the data to the broker.
2. The database *subscribes* into the Broker in order to periodically keep track of the retrieved data.
3. The server *subscribes* in the Broker and *receives* the published sensors data.
4. The web server, including smart applications, *presents* the appropriate command, and *pulls* it onto the MQTT Broker.
5. The actuators *subscribe* in the Broker then it *receive* and *execute* the commands.

6. The application *retrieves* or *updates* the database values.

7. External actors, through web and smart applications, communicate securely with web server by encryption method like RSA.

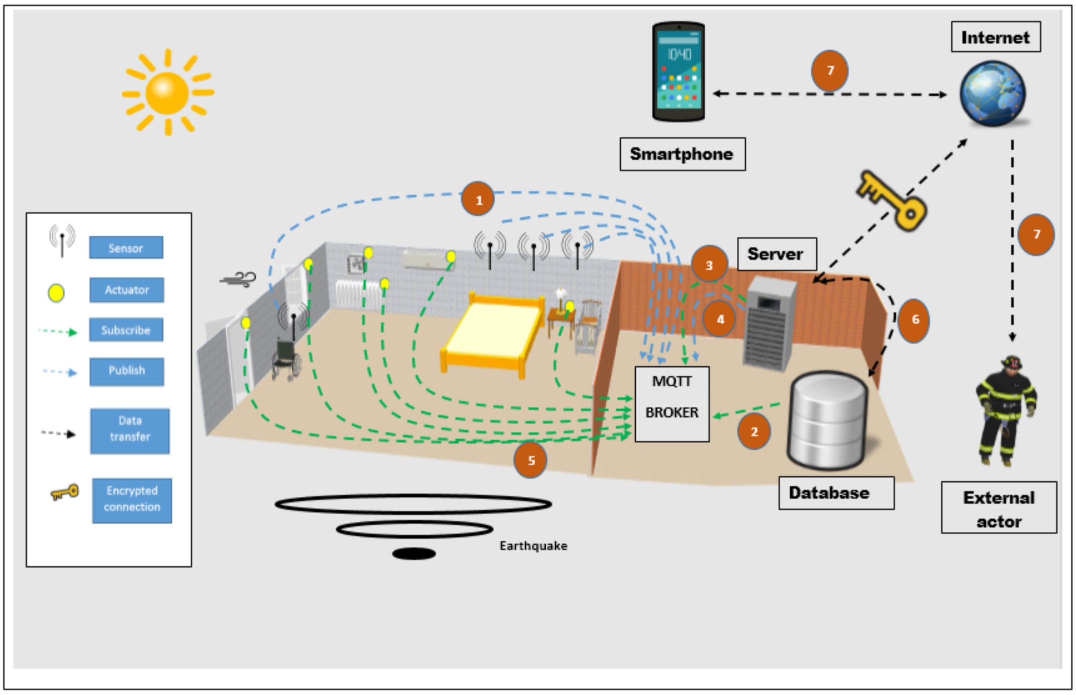


FIGURE 3.2: The communication steps.

3.4 Experimental Results

In this section, we show the effectiveness of the proposed framework on two real cases scenarios. As mentioned, we use Uppaal, an integrated tool environment for modeling, validation and verification of real-time systems modeled as networks of timed automata extended with data types. For each real scenario, we instantiate from the predefined state machines the proper ones for each scenario. The first scenario shows the correct functioning of the architecture, and it is about how it reacts in case of a fire (for example) and the second is about security.

The first scenario: here, we will check a general case, where a fire is in a smart room, and we will look to the reaction of sensors, then we exploit collected information submitted to server and smartphones, and also retrieved data from database. The scenario is unfolded as follows.

1. We turn on all smart room device, and we make both the server, database, and actuator subscribe in the Broker to receive the acknowledgment messages from it. Then, we make the Smart-phone authenticate to the server in order to exchange the messages between them (client-server).

2. We increase a parameter that represents the degree of smoke, and when it is greater than or equal to a threshold already defined, the condition which identifies that there is a fire is verified, then the sensor goes to the transmission state after sending a message to Broker.

3. When the Broker receive the message, it sends values to database to store current changes, and it sends to the server if the last two machines are subscribe in Broker, else the transmission process will be stopped.

4. When the server receive the message, it discover its type (Broker message), it reacts with the new value and it delivers a signal command to the Broker. As the smart-phone authenticate to the server, the server can send an encrypted alert message to it.

5. Broker passes the command to the specified actuator according to the topic, and as a result, it will be in the action state.

6. At this point, we test the ability of the smart-phone to access and retrieve the stored values from the database, as also the user wants to see the history events recorded within a period of time. So the Smart-phones send an encrypted select command to the Server.

7. The server checks the command and the authentication of the Smart-phone, if they are true it receives the command and delivers it to the database in the form of SQL command, else it stops the transmission process.

8. When the database receives command, it detects its type (select command), then it sends the data to the server without changing the stored data.

9. The server receives the database request, then it sends to the smart-phone the encrypted request that allows the smart-phone application displays the message after decryption.

10. Then, the smart-phone wants to update the data in the database. To do that, the smart-phone sends the encrypted message to the server if it is authenticated.

11. The server receives the command and identifies its type of command. Then it decrypts the message and delivers the SQL command to the database.

12. The Database detects the update command and resends the data to the server with changing of data stored in the Database.

13. The server receives Database request, then it delivers to the Smart-phone his encrypted message to inform the user of access the operation, The Smart-phone decrypts and displays the message.

The second scenario: This part checks the exactitude two security concepts (see the figure 3.3).we check the confidentiality of information published by the broker and the subscribe objects (server in this case).

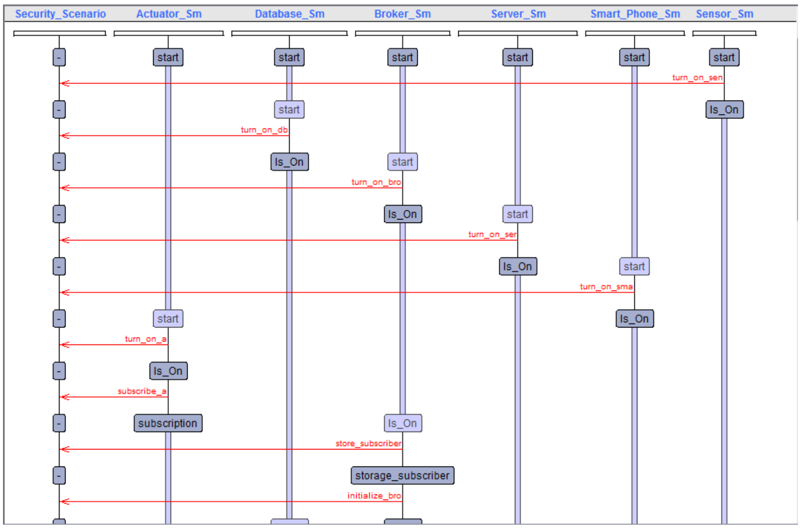


FIGURE 3.3: The simulation of the security concept.

1. Turn on all smart room devices, we make the smart-phone authenticates into the server, and for the subscription in the broker we only subscribe both the database and the actuator (without server).

2. We increase a smoke parameter to move the sensor detection state then publication state.

3. The broker sends the received information only to the database.

4. The server cannot receive the information from the broker, because it has not subscription in the broker.

From this experiment results, we observe that the states machine work very well, together and in communication. All scenarios progress without deadlock and with a correct behavior. We conclude that all state machines form a correct and complete system, they execute without errors, and easy to deploy.

3.5 Smart Building Case

For a better living quality, the smart spaces paradigm aims at constructing advanced service infrastructures that follow the ubiquitous computing approaches where smart objects are executed on a variety of digital devices and services are constructed as interaction of agents in a communication environment [158]. Recent advances in intelligent computer systems and communications have created the necessary conditions for the networking of a wide variety of heterogeneous devices. This led to the integration of short-range mobile transceivers into everyday life objects and has enabled new forms of communication between objects and even between people and objects. The concept of smart devices, i.e. the inclusion of software, identifiers and networking to devices typically not computerized, led to the "Internet of Things" (IoT) [176]. The main feature of this technology is the integration of heterogeneous and action elements (actuators) in a distributed system which performs different actions based on the information gathered by the sensors combined with the requirements of the particular application [159].

The inside environment has several factors that can affect it or the life of inhabitants or both at the same time (temperature, humidity, noise, light, *etc*). Nowadays different numerical models are available to describe the vapor balance of transient water in a room and predict indoor humidity. A typical room moisture balance includes water vapour production by moisture sources (humans, plants,...), convective water vapour transfer with ventilation air, and water vapour exchange with the building fabric and furniture.The water vapour exchange between room air and surrounding materials (walls and furniture) is governed by three physical processes: the transfer of water vapour between the air and the material surface, the moisture transfer within the material and the moisture storage within the material. The existing models mainly differ in the way this last part of the moisture balance is described [160]. In general, sensors communicate directly with the home gateway and feed the system information with regards to the obtained environment measures, for example light intensity inside a particular room, temperature inside and outside the home and motion sensing to name a few [161].

In this chapter, we propose a smart living framework by modeling the different components needed for an indoor environment and developing a trustworthy architecture that ensure the well functioning correctness of such system, and also its configuration and control. First, we rely on the existing limitations and the requirements for a home that can affect the inhabitant like humidity which causes corrosion coating of the wall and household furniture, the appearance of molds and bacteria, the temperature also has to be regulated in the home according to the outside climate, loud noise especially at night, the handicapped can not open the doors of the room, natural and artificial phenomena such as the earthquake and fire that threatens the life of the human. The proposed solutions consider all indoor issues, implement sensors for each measure, collect data in real time and make reactions to prevent risks.

The proposed framework is a web service based solution where sensitive nodes are indoor planted and their measures change in real time. The architecture proposed for the framework considers different classes of nodes. A database node containing the collected data by sensors, a server node that ensures the communication and the reliability between nodes, and reacts when necessary by sending the appropriate control commands; the actuator node executes the received commands from the server and/or external actors who can extract or edit home data. The architecture uses MQTT protocol [162] to ensure a reliable communication between the predefined internal nodes. Further, the architecture implements a precise constraints and requirements for the communication and during executing actions. Otherwise, the nodes do not respecting certain conditions are considered as unacceptable nodes. Finally we ensure the functional correctness of the nodes and their secure communication by simulation and verification in Uppaal tool [163]. The results show that the proposed framework is a deadlock free, secure, and respecting the indoor living requirements.

Figure 4.1 illustrates the steps to how construct a secure smart building/home system and analyze it. The system's architecture is composed from a set of nodes, security constraints and management mechanism, and the communication protocols. The nodes are active/passive objects to collect the needed environment measures. The communication protocols ensure how well the connection between nodes is established and the measured data are packed and encrypted. The security management mechanism reinforces the architecture in order to create a protected system.

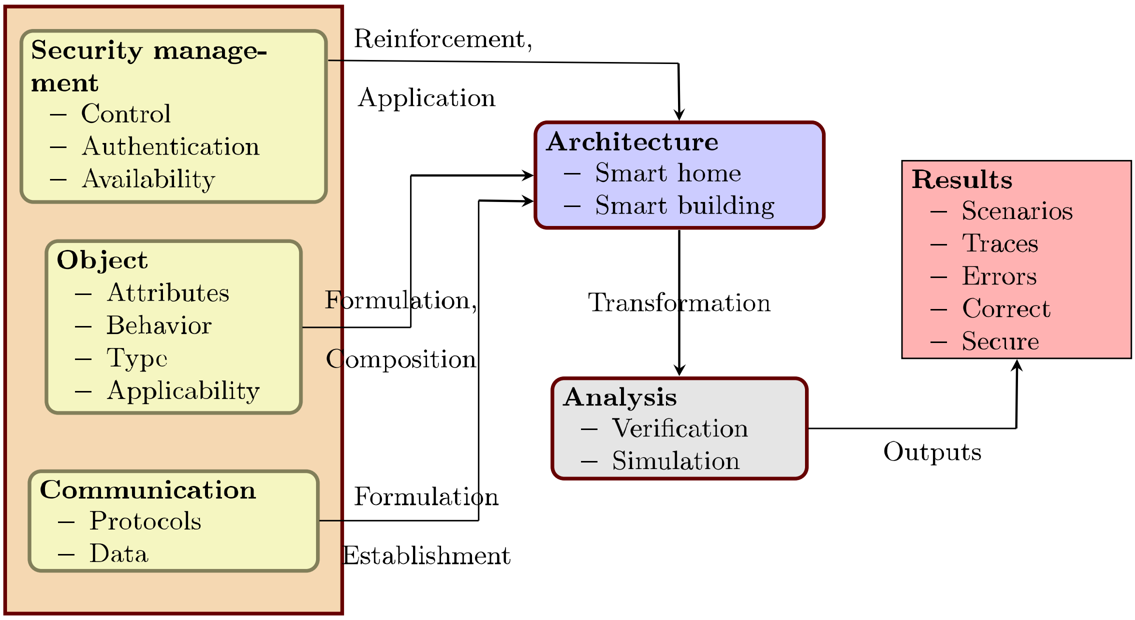


FIGURE 3.4: A Security and Analysis Framework for Smart Homes and Buildings.

It develops a set of security rules including the authentication and identification of nodes, the control access, and how to keep the availability of services. The analysis step enables the verification of the accuracy of the implemented architecture with respect to the security rules. Finally, the results show the different scenarios, traces, or errors that might affect the security and the well functioning of the architecture in order to decide or not its deployment.

3.5.1 Smart object

A smart object ($\texttt{SoT} \in \textbf{SoT}$) is identified by a set of dynamic and static attributes ($\texttt{T}$). The dynamic attributes are classified into two categories: data ($\texttt{d}_i$ of type real) and flags ($\texttt{f}_i$ of type Boolean). In the following, we cite the most used static attributes that describe the physicality and the technicality of an $\texttt{SoT}$.

- The identifier ($\texttt{id} \in \texttt{ID}$): is the unique reference to $\texttt{SoT}$, in our case $\texttt{id}$ is IPv6 [164].
- The connectivity ($\texttt{COn} \in \texttt{T}$) describes when devices have extensions to connect to each other [165].
- The battery life ($\texttt{BLi} \in \texttt{T}$): represents the longevity of a battery [166].

- Powered by electricity (`PEl` $\in$ `T`): when `SoT` can be plugged with an electricity line.
- Data security (`DSe` $\in$ `T`) informs about the ability to encrypt informations stored or sent [167].
- Small size (`SSi` $\in$ `T`): describes the volume of `SoT`.
- High product quality (`HPr` $\in$ `T`) indicates the possibility to increase the service life and to reduce the cost of maintenance.
- Constrained device (`CDe` $\in$ `T`) describes if a cheaper device can cover a specific space[168].
- Price (`PRi` $\in$ `T`) helps in the budget management[169].
- Service availability (`SAv` $\in$ `T`) to check if the device works continuously or not [170].
- Minimum error (`MEr` $\in$ `T`) increases the quality of service [171].
- Easy to maintain (`EMa` $\in$ `T`) is to reduce time, effort and the cost of maintenance.
- Required a low connection rate (`RLo` $\in$ `T`): to stay connected in the worst case [172].
- Interoperability of nodes (`INo` $\in$ `T`) defines the technologies supported by the node [173].

The behavior of an object is the effect of the executed actions (Σ) that allows it to transfer from its current state S_i (the evaluation of dynamic attributes) to another one S_j. The following lists the set of possible actions.

- `turnOn/turnOff` to turn on/off the smart object [174].
- `send/receive` to send/receive data to/from another IoT node [175].
- `collectData` to collect the received information [175].
- `applyAction` apply an action after getting command [175].
- `encrypt/decrypt` to encrypt/decrypt a message.
- `authenticate` grants the possibility to send data.

We define in Definition 3.5.1 a smart node that can be a sensor, actuator, broker, database, server, or smartphone.

[Smart node] A smart object $\texttt{SoT} \in \mathbf{SoT}$ is a tuple $\langle \texttt{ID}, \texttt{Att}, \Sigma, \texttt{B} \rangle$ where:

1. $\texttt{ID}$ is a finite set identifiers $\texttt{id}_\texttt{i} \in \texttt{ID}\{O_i, i \in N$ where $\texttt{id}_\varnothing \in \texttt{id}$ is an empty object.

2. $\texttt{Att} : \texttt{ID} \rightarrow 2^\texttt{T}$ is a function that assigns for each object a sequence of attributes.

3. Σ is the set of possible actions for an objects,

4. $\texttt{Beh} : \texttt{ID} \rightarrow \texttt{B}$ returns the expression that precises the behavior of an object in the dominant case where : $\texttt{B} ::= \texttt{Start.actions} +_\texttt{g} \texttt{actions.}\mathrm{End}$ where $actions = \alpha | \alpha.actions$ such as $\alpha \in \Sigma$ and $+_g$ is a deterministic choice with respect to a guard g.

[Smart object] Based on Definition 3.3.2, the semantics of a general sensor is the state machine depicted in Figure 3.5 where states s_0, s_1, s_2, s_3 stand respectively for *Is_On*, $detection$, $declaration$, Is_Off. The attributes values specifying a state change regarding the executed action. The actions α_1, α_2, α_3, α_4, and α_5 represent respectively turn_on, detect , send,turn_off, and initialize.The dynamic attributes ($\texttt{d}$ and $\texttt{f}$) of a sensor are: $\texttt{d}_1$ evaluates the energy, $\texttt{d}_2$ measures other properties (smoke, noise, temperature,...), $\texttt{f}_1$: detection, $\texttt{f}_2$: availability, $\texttt{f}_3$: alerte_msg. Each state is presented by the following predicates where *Max_Val* is the maximum for the measure related to the smart object.

1. $[\![s_0]\!] = (\texttt{d}_1 > 0) \wedge (\texttt{d}_2 < Max\_Val) \wedge (\neg \texttt{f}_1) \wedge (\texttt{f}_2) \wedge (\neg \texttt{f}_3)$

2. $[\![s_1]\!] = (\texttt{d}_1 > 0) \wedge (\texttt{d}_2 >= Max\_Val) \wedge (\texttt{f}_1) \wedge (\texttt{f}_2) \wedge (\neg \texttt{f}_3)$

3. $[\![s_2]\!] = (\texttt{d}_1 > 0) \wedge (\texttt{d}_2 >= Max\_Val) \wedge (\texttt{f}_1) \wedge (\texttt{f}_2) \wedge (\texttt{f}_3)$

4. $[\![s_3]\!] = (\texttt{d}_1 = 0) \wedge (\texttt{d}_2 = 0) \wedge (\neg \texttt{f}_1) \wedge (\neg \texttt{f}_2) \wedge (\neg \texttt{f}_3)$

3.5.2 Smart environment

We define a smart environment $\texttt{sEnv}$ as a structured physical infrastructure, building or home, that carries smart nodes. $\texttt{sEnv}$ is composed of at least two smart rooms/locations disjointed by separators *like* walls, doors, and windows. To collect information and sensitive data, smart nodes are

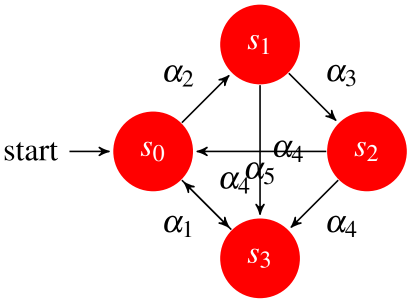


FIGURE 3.5: The state machine of a sensor.

connected with a precise architecture mechanism that helps them to communicate easily through a dedicated protocols.

[Smart Environment]

A smart environment `sEnv` is a tuple of $\langle E, L, \mathbf{SoT}, \mathtt{pl}, \mathtt{dl} \rangle$, where:

1. E is the environment name/id,

2. L =$\{R_1, ..., R_i, ..., R_n | i, n \in \mathbb{N}$ } is the set of locations/rooms (R_i) composing E,

3. **SoT** = { $\mathtt{SoT}_1, ..., \mathtt{SoT}_\mathtt{m} | \mathtt{m} \in \mathtt{N}\}$ is the set of smart nodes in E,

4. PL = { $pl_1, ..., pl_n | n \in \mathbb{N}\}$ is the set of physical structure that defines E,

5. DL = { $dl_1, ..., dl_n | n \in \mathbb{N}\}$ is the set of logical architecture that connects **SoT**.

Figures 4.2 and Figure 4.3 show respectively an abstraction of the physical structure of E and the logical architecture between nodes in E.

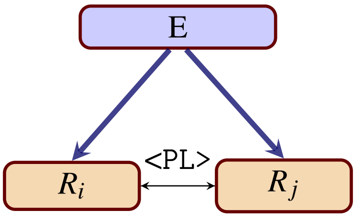


FIGURE 3.6: The physical structure of E.

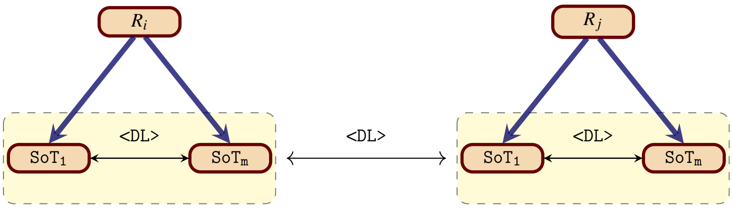


FIGURE 3.7: A Logical/Digital structure in E.

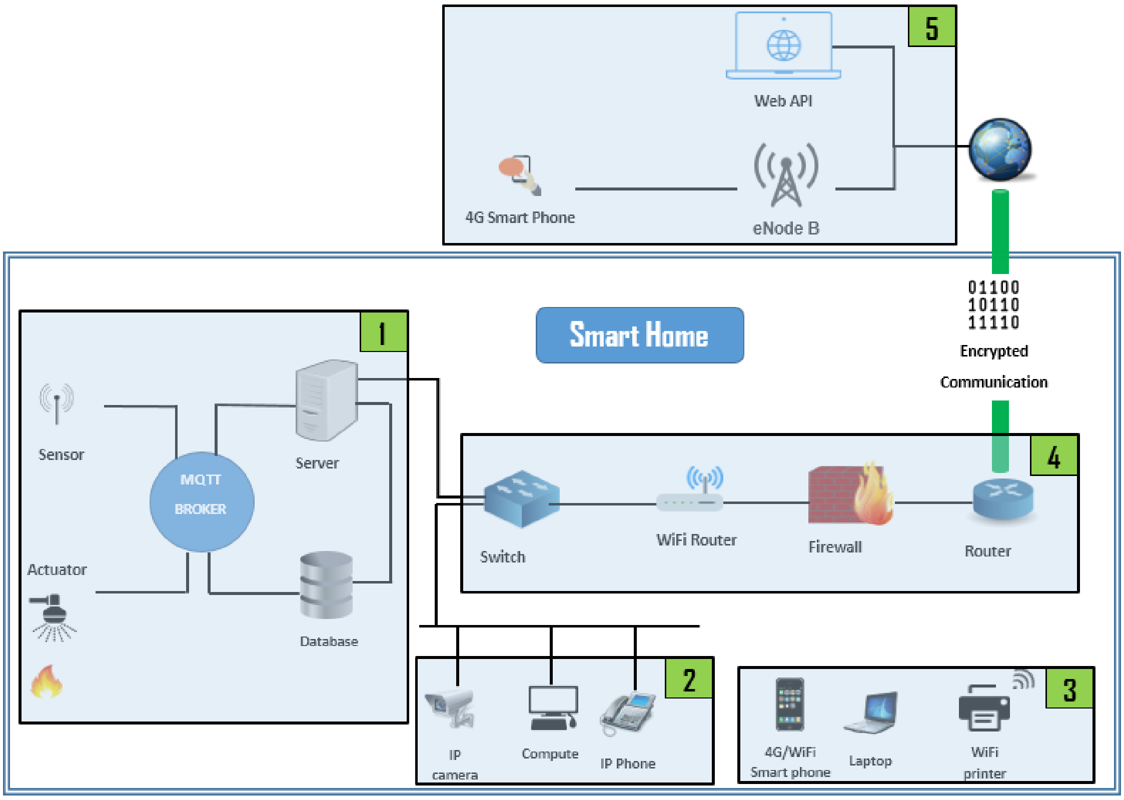


FIGURE 3.8: The architecture of Smart Home

3.5.3 Architecture

The architecture is grouped into five main levels depicted in Figure 3.8:

The first is the most important because it contains sensors that capture the state of smart home periodically then they report if there is a contradictory case (fire, humidity, high temperature, ...), the analysis devices as the database, web server and broker save or process the signals of the sensors then give the actuators the commands to do the necessary actions.

The second level is the set of objects referenced by an IP address linked with the router by a network wire; they can access the internet connection. The third level is IP objects use wireless technology like Wi-Fi, Bluetooth, 4G...

The fourth level has processing devices like router, firewall and switch, they are used to make an interconnection between smart home objects and they are like a point between the outdoor and indoor smart home.

The fifth level is the set of APIs and devices outside smart home that can access the smart home interior objects.

3.5.4 Communication

In this part we will present some protocols that can be used in the proposed framework that deals with architecture as the one showed in Figure 3.9. Herein we present the adopted protocols by the framework.

MQTT

It is a machine-to-machine connectivity protocol designed as an extremely lightweight publish/-subscribe messaging transport [177]. The operations of this protocol passes through steps shown in Figure 3.9, where it is applied on Smart room, and it is the first level represented in the architecture.

1. A sensor collects information (temperature, fire, humidity, etc.) then it *publishes* the data to the broker.

2. The database *subscribes* into the Broker to store the information that can be study in future, e.g. If a fire is repeated at a specific time, the protection will be strengthened at this time.

3. The web server *subscribes* into the Broker and *receives* the published sensors data. , the server can be supported by algorithms that process the flow of data collected, e.g. in fire case, it send an email to fire station, and inform user.

4. The web server, including smart applications, *presents* the appropriate command, and *pulls* it into the MQTT Broker.

5. The actuators *subscribe* in the Broker then it *receive* and *execute* the commands.

6. The application *retrieves* or *updates* the database values.

7. External actors, through web and smart applications, communicate securely with web server.

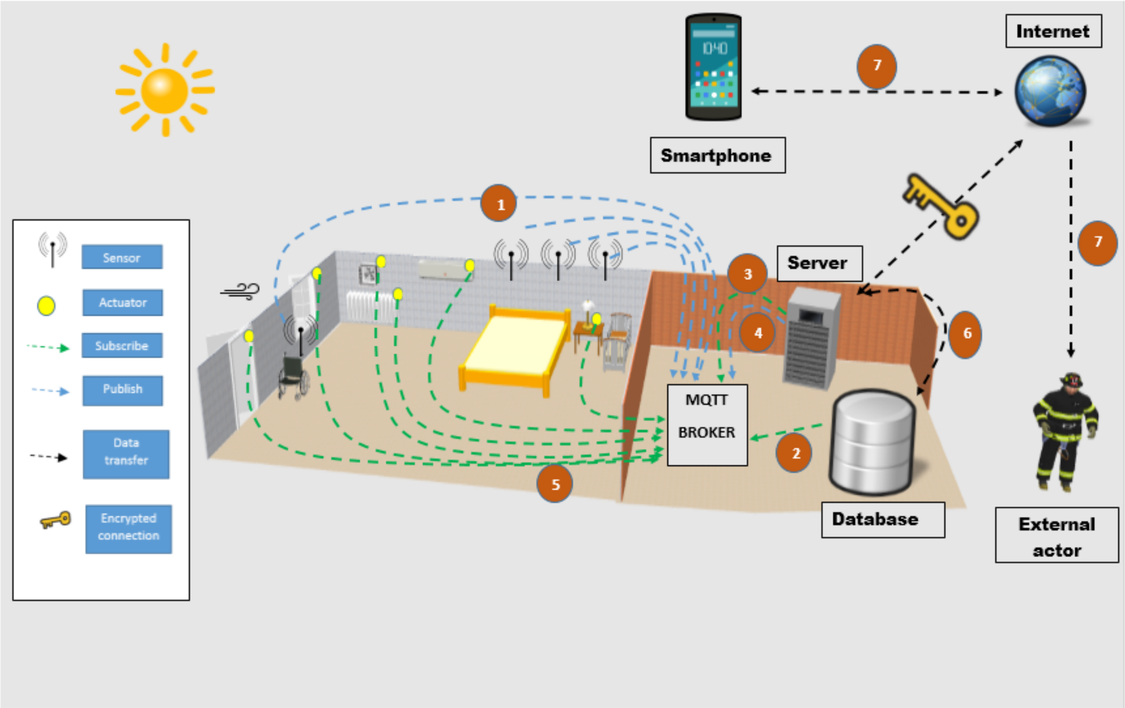


FIGURE 3.9: Operation protocol MQTT in architecture.

ONVIF

It is used to establish a communication between the network camera and a point outside the building in order to monitor its status in real time.

Http

People authenticated in the web server can access through an API that uses this protocol to view or edit information about the building.

VoIP

Phones equipped with a network card can make calls using this protocol.

Ethernet

It is a data link layer protocol in the Open Systems Interconnection (OSI) model that allows objects affiliated with the same LAN to interchange data.

3.5.5 Security

The digital environment always at risk, for this we rely on the security side in our approach to avoid information theft, data interception or disservice. We consider the following five concepts in order to stop or decrease threats.

- **Confidentiality**: ensure that each data access only by objects (people, devices) that we define them through encrypting data with a strong encryption method. Ignoring this principle can cause a destruction of information.

- **Authentication**: Some smart home objects (such as the server) request objects that want to access it to define its identification in order to prevent unauthorized access.

- **Data Integrity**: Man in the middle [178] can intercept the flow of data between IoT objects, change it then send it back to the receiver. So we use some mechanisms like hashing [179] (MD5 and SHA-2) and electronic signatures [180] to control if the message is changed or no.

- **Access control**: Smart home objects with their security levels allow functions according to a predefined authorization and prevention rules. The architecture supports firewalls [181] at the gateway level that manage the input and output packets. Further, for security policies we are interested in access control mechanisms [182] (RBAC) and adapting the router by an access control list ACL [183].

- **Non-repudiation**: Since IoT objects always in contact it is important to check the legitimacy of the sender and the receiver. The most able method to realize that is the electronic certificate [184].

3.6 Experimental Results

To test the accuracy of the proposed, we built it within the validation and verification tool Uppaal, by integrating the machine states of smart objects and create the smart home architecture where the smart home objects (composition of states machines) react. The logic behind this composition ensures that the proposed framework does not oppose the requirements. First we ensure through simulation then verification. The simulation is partitioned in four phases, the first tests the operations of MQTT protocol, the second tests the connectivity with a external point, the third tests for exceptional cases where IoT devices can not connect to each other and finally we verify the satisfaction of the security rules that we must respect in the proposed system.

3.6.1 MQTT protocol test

We test the MQTT protocol via a scenario simulates the case of fire in smart home, the first scenario steps are presented in the Figure 3.10, our system function without deadlock.

3.6.2 Connection with distant points

The distant smart home users use IoT nodes to access smart home objects via the internet connection. In this point we will study two examples, the first is a user that accesses by his smartphone to the smart home server in order to extract data from the database, and the second is a web API accesses to a Webcam Home, system operation does not give errors.

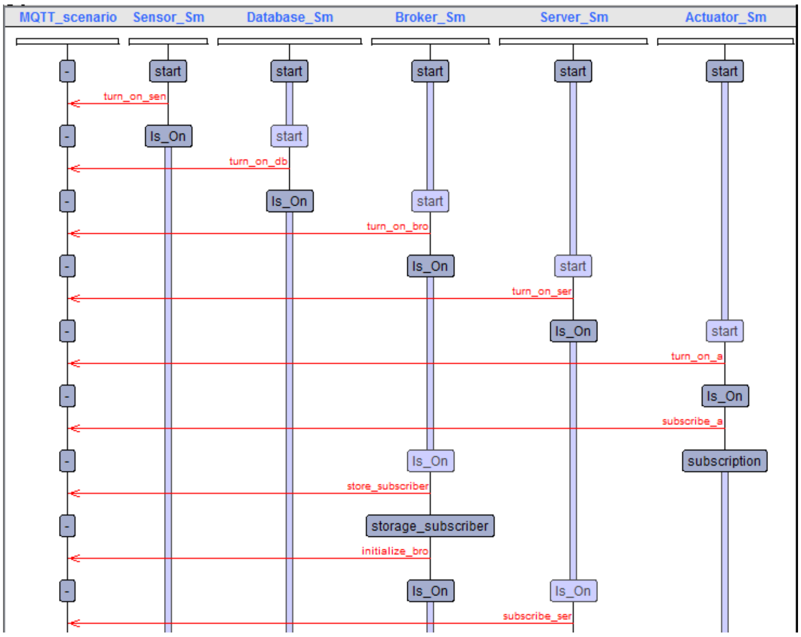


FIGURE 3.10: MQTT Simulation Scenario.

3.6.3 Exceptional cases:

The nature of these tests simulates contradictory cases that affect the exchange of messages, in this test we check the operation of system with three cases contradictory with the natural operation(Webcam not linked, Firewall prevents webcam contact and The API does not authenticate the webcam), the resulat was that the test procedure is not finished.

3.6.4 Security rules verification

Uppaal has a language called ’query language’ which allows to edit rules after the construction of states machines of the objects to test the accuracy of these objects. The language is written according to specific norms and symbols.To verify the security rules, we express the query language to check these goals Confidentiality, Authentication, Data Integrity, Access control and Non-repudiation. The verification results show that all the security rules are checked and satisfied.

3.7 Smart City Case

Cyber-Physical Systems (CPS) are combination of computation with physical processes. Embedded computers and networks control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. It has many application domains including transportation, healthcare, industry, buildings, and cities [185].

A smart city may be a well-defined geographical area during which information and communication technology, logistics, and energy production can cooperate to get benefits to residents regarding comfort, tolerance and participation, environmental quality, and smart development. It is controlled by a well-defined subjects that provide the city government with a set of rules and policies (Figure 3.11) through analysing the different parameters using IoT devices such as sensors [186].

UNESCO[5] stated that through innovative urban systems, smart cities play an important role in socio-economic development while improving people's lives [1]. Also, UNECE [6] asserted that a smart sustainable city is an innovative city based on ICTs (Information and Communication Technologies) and other technologies to optimize quality of life, the efficiency of urban operation and services, and competitiveness [2]. A smart city [3–5] is defined as a wide area occupied by citizens, and divided into many smart components such as smart buildings, smart ICTs, smart transportation, smart health, smart grids, and other services. It supports a hierarchical network model, where the data captured can be published, stored, and analyzed [6].

In an IoT model, objects will make the smart city as a single interconnected network. Information and communication systems will be integrated within the smart city, in addition to a large distribution of Radio Frequency IDentification (RFID) and sensors technologies. This results in huge amounts of data, which must be stored, processed and presented in a smooth and reliable manner. The model will consist of services where commodities are provided in a traditional way [187].

Internet of things (IoT) is a network that combines physical components as sensors, smartphones, servers, etc, with the ICTs to sense in real-time the environment's measures, process the collected data, remotely control and make decisions, etc. The IoT network is characterized by low cost, large coverage, high secure level, scalability, and low latency. However, IoT is used in diverse applications domains like modern cities, industrial, home appliances, healthcare, transportation, sensors development, emergency, and other cases. It adopts some communication protocols and information sensing equipment to achieve smart deployment, controlling, and monitoring resources

[5] United Nations Educational, Scientific and Cultural Organization.

[6] United Nations Economic Commission for Europe.

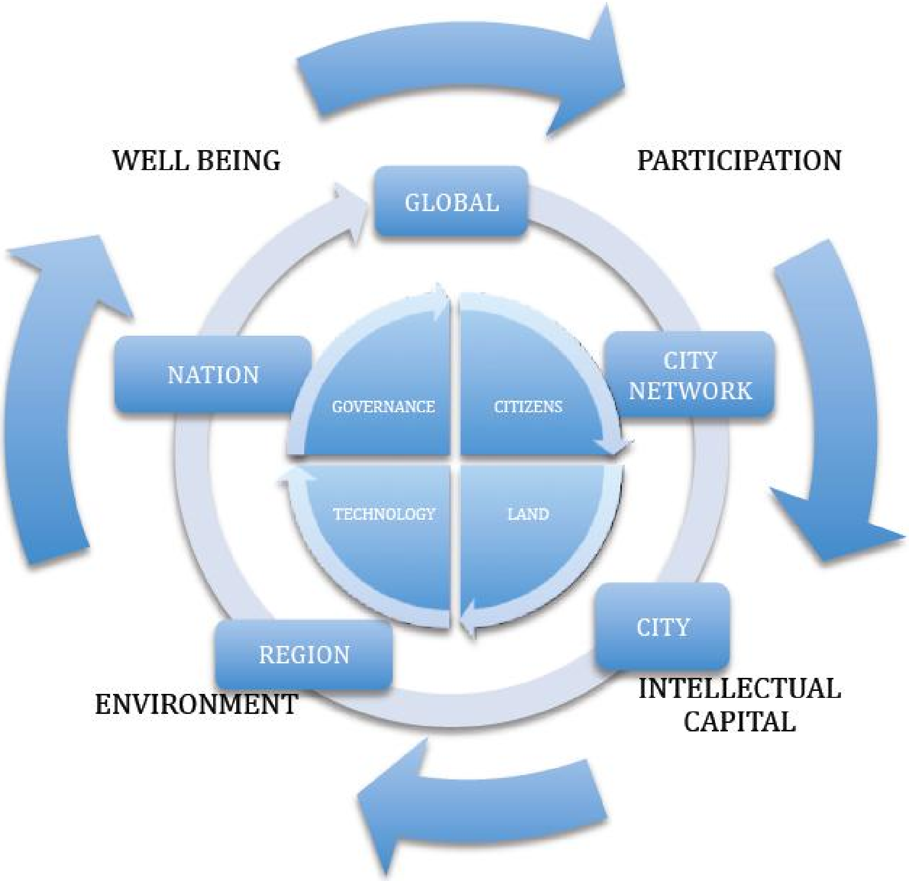


FIGURE 3.11: Smart city comprehensive schema [186].

in real-time [188] while respecting the security standards and measures [189]. For a reliable network, the data flow traffic is distinguished by the automated process, where the analysis level treats the received data from the sensors and makes the decisions through machine learning-based supports. However, the adopted technologies should be *"secure, flexible, extensible, and sustainable"* [190]. Further, the used protocols in smart cities are different.while IoT devices are featured by the low memory and low processing of data.

Many challenges are facing smart cities such as safety, security, energy, coverage, etc. For example, the energy consumption is estimated to be increased by 32% [191]. Hence, the lifetime of a building network relies on the quantity of energy provided to the smart appliances, the characteristics of the object that may cause high consummation, the used communication protocols, and the number of operations applied in the network. Also, the increasing demands for internet services cause the high latency, which impose us to integrate technologies of higher band-width to achieve higher data transfer. In addition, cyber risks are a big problem in the IoT paradigm since the cyber security standards do not cover precisely sensors and objects, and therefore it is difficult to monitor the corporations that provide IoT services [192].

However with any system, before deploying a concrete smart city, it is necessary to design its components and their relations, as well as ensure their functional correctness. Farther, such design dedicated to a smart city should achieve its main requirements, especially: safety, low energy consumption, low latency, network interconnectivity, and scalability. This chapter develops a framework to ensure the good development of a more secure and reliable smart city by:

1. Designing a secure and robust Smart City Model (**SCM**) that can be integrated within the building information model (BIM).

2. Developing a formalism dedicated to smart cities by enclosing their different digital and physical components. It includes also their connection supports and adopted communication protocols.

3. Proposing an hybrid approach that is based on formal methods and network analysis to analyze the correctness of the designed **SCM**.

4. Enhancing the security level of **SCM** by proposing a set of access control policies and a dedicated algorithm to protect objects from unauthorized access.

5. Proposing the use of temporal logic formalism to express **SCM** requirements.

6. Using the Cooja simulator to check the connectivity and energy consumption in **SCM**, the Uppaal model checker to verify the correctness of **SCM** and how well the security access policies are respected.

This section covers the proposed framework to create a realizable smart city model. As depicted by Figure 4.1, it starts by creating the smart city model that includes both **P**hysical **M**odels (**PM**) and **D**igital **M**odels (**DM**), where both models contain ingredients that are detailed textually and formally. The analysis step checks, then it validates how well **SCM** models are functionally correct through verification and simulation techniques. This step considers the developed **SCM** models as a network of Timed Automata (TA) and expresses the **SCM** requirements as TCTL [7]

[7] Timed Computation Tree Logic

formula [193]. Hence, the Uppaal model checker is used to check if the requirements are satisfied, or not. Consequently, the Cooja network simulator previews if WSNs achieve a low consummation of energy with high coverage of the area of interest. If the outputs obtained from this step declare errors, it is necessary to return to the previous step in order to rebuild the **SCM**, else the verified model has the ability to be deployed in the BIM and the area of interest.

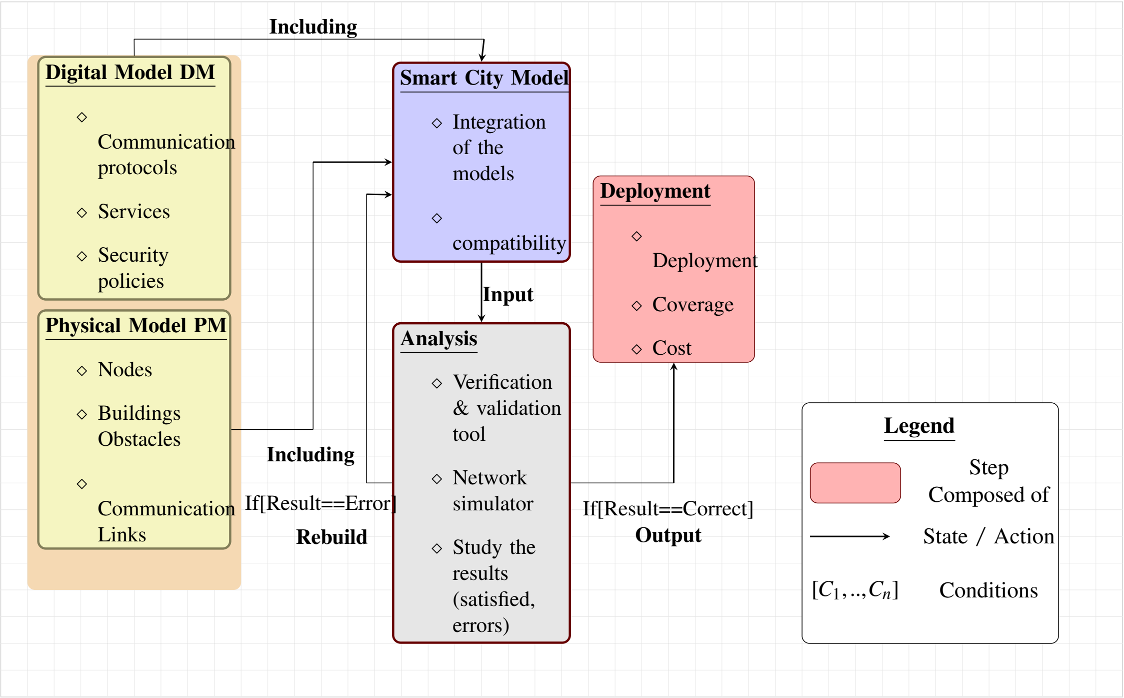


FIGURE 3.12: The methodology to construct SCM.

3.7.1 Smart City Model

Our proposed **SCM** architecture is divided into three levels (see Figure 3.13). The third level is dedicated to processing and storage services by including different resources such as the servers and calculators with software to receive, process, and share data (e.g., a server receives and processes the temperature measures that are captured by sensors, then gives the appropriate control commands). Since this level deals with sensitive data, we isolate it through three cloud services: *Saas* (Software as a service), *Paas* (Platform as a service), and *Iaas* (Infrastructure as a service) [194]. Physically, there is a long distance between the first and the third level components, e.g. when the request is forwarded from the *third* level devices to the cloud computing server. The transmission will have a high latency, which is one of the basic requirements in IoT systems. To resolve the latency issue, we add fog computing [195] to the third level that is located close to the lower levels. Thus, the “most used services” are installed in the fog whereas the "less-used services" are in the cloud. In addition, in order to serve the first level requests, a set of servers are equipped in this level e.g., Web servers, FTP, Mail, etc.

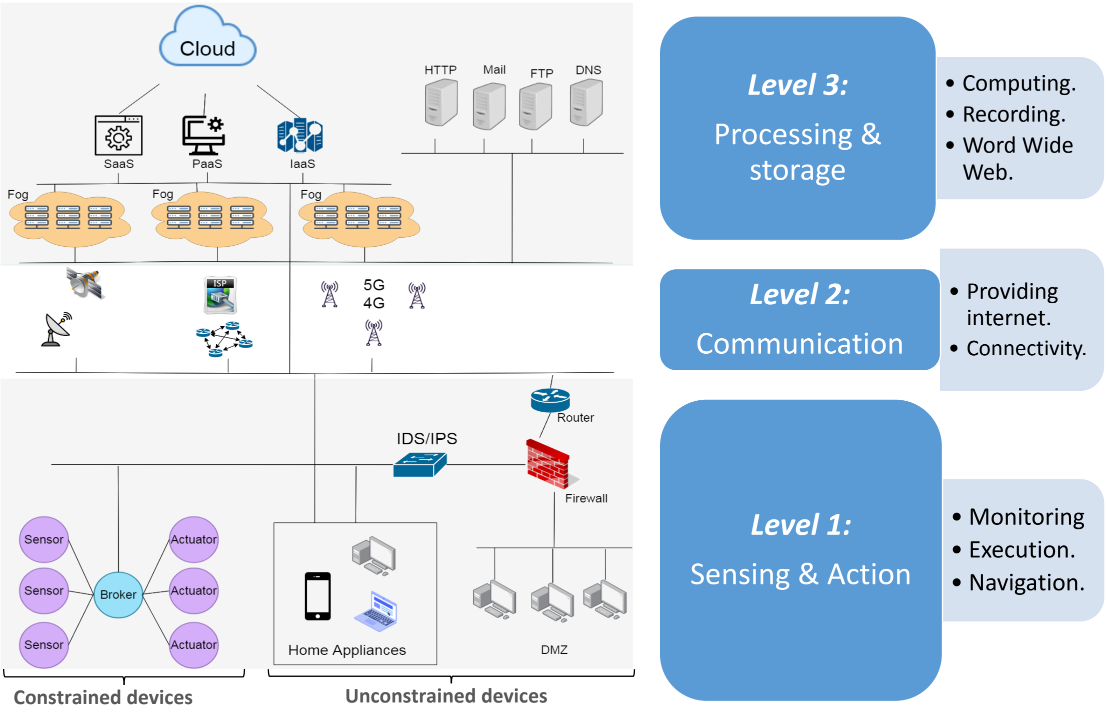


FIGURE 3.13: Smart City Architecture.

The second level (**Communication**) is a collection of internet stations and providers to link the other levels. It includes ISP (Internet service provider), 5G Mobile Broadband Providers, and Satellite Internet Providers. The quality of services is related to the type of internet providers, so, the differences among them are due to the differences in the variables: latency, coast, coverage, security, etc. For example, 5G technology is a fast-wireless communication, ADSL is more reliable, satellites provide coverage in the worst places.

The first level (*Sensing and Action*) is the indoor sub-architecture secured by hardware and software tools. The firewall is a necessary device to filter the input/output data and to construct sub-architecture as the Demilitarized Zone (DMZ)[196]. The Intrusion Detection System (IDS)

[197] or Intrusion Prevention System (IPS) [198] are installed to detect and prevent BIM's intrusions. It contains unconstrained devices [8], that are responsible to monitor and request data (like computers and smartphones) through different protocols: HTTP, FTP, SMTP, POP,and others. Further, this level has constrained devices [9], especially sensors to monitor and share the conflicting changes in the environment (such as temperature, movements, noises, fire, etc.). We classify two types of sensors, wired sensors and Wireless Sensors Network (WSNs). The latter are the most important since they are mobile and support many IoT communications protocols like (Zig-bee, Bluetooth low energy, IEEE 802.15.4e, RPL, etc.). In addition, the actuators are objects that receive the commends and execute the appropriate actions (like turn on the air conditioner, open the door, etc.)

We consider an **SCM** as an association that brings together both the digital and physical models (Figure 3.14).

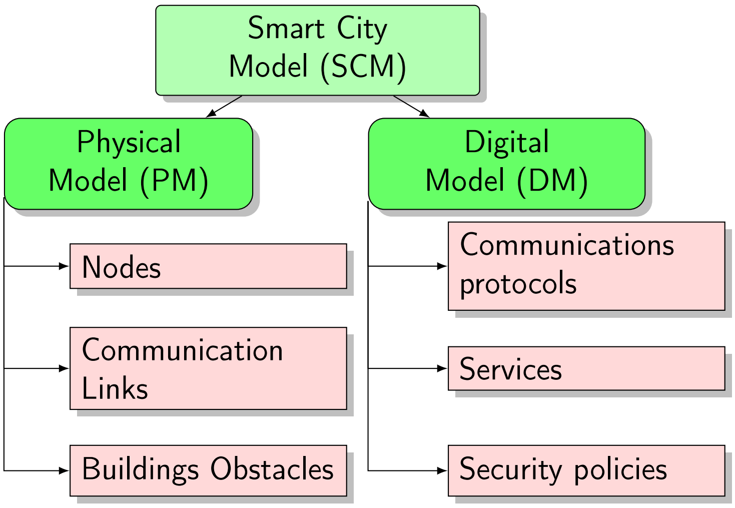


FIGURE 3.14: Smart City Model.

3.7.1.1 The Physical Model (PM)

PM is a set of hard components that visually construct the concrete building/city, and it includes:

[8] Devices that are characterized by large memory and processing capacities.

[9] Devices, that are characterized by low memory and processing capacities.

Nodes.

They are a set of sensing, application, processing, routing, and storing appliances such as sensors [199], actuators [200], servers [201], routers[202], and data center [203]. We define a *Node* by the tuple $\langle attr, action, State, Behavior\rangle$, where: *attr* is a set of *static* and *dynamic* attributes evaluated by the value *val*. The "*static*" attributes are fixed while a node is running, *e.g.* the size of an object, memory capacity, etc. The *dynamic* ones change when a node executes its proper *actions*, e.g, the battery degree, availability (On/Off), etc. The evaluation of *attr* by *val* can be real or boolean. *action* is the functions that take a set of parameters $IN \subseteq attr$ as input to evaluate the node attributes "*attr*". Its execution produces the changes in the output parameters: $OUT \subseteq attr$, $action : attr \rightarrow attr$ where $action(IN_i, ..., IN_n) = \{OUT_j, \ldots, OUT_m : i, n, j, m \in \mathbb{N}\}$. A given *Node* can execute during during its life cycle (see Figure 3.15) the following actions: $Turn\_on(), Turn\_off(), Send(), Receive(msg), Store(info_1, .., info_n), Process(info_1, .., info_n)$, $Charge\_power()$, and $Consume\_energy()$.

A $State_i \in State$ defines the status of the *Node* when an *action* is applied and characterized by the evaluation of its proper attributes given by $State_i = (attr_1 = val_1) \wedge \ldots \wedge (attr_n = val_n)$. Furthermore, *Behavior* of a *Node* is a timed automata showing the changes of its "*state*", where : $Behavior = State \times action \times State$.

Example 3.16 shows the timed automata of the fire sensor *node*. In the *on* state, it measures the conflicting changes (degree of the smoke) in the air. If this measurement exceeds a predefined threshold parameter, the sensor sends an alert message to the receiver *Node*. The sensor will be out of order if it is turned off. This *action* includes the process of turning off or running out of power in the battery.

Connection links

They are the wire or wireless *links* that relate nodes through their ports. $connection = \langle N, L\rangle$ is a direct graph (see. Figure 3.17), where: N is a set of *Nodes*, and L is the set of *Links* relating *Nodes*, given by $L \subseteq \{(x,y)|(x,y) \in N \times (N)\, and\, x \neq y\}$, the pair (x,y) indicates that the *Node* x has the ability to send a message to the *Node* y.

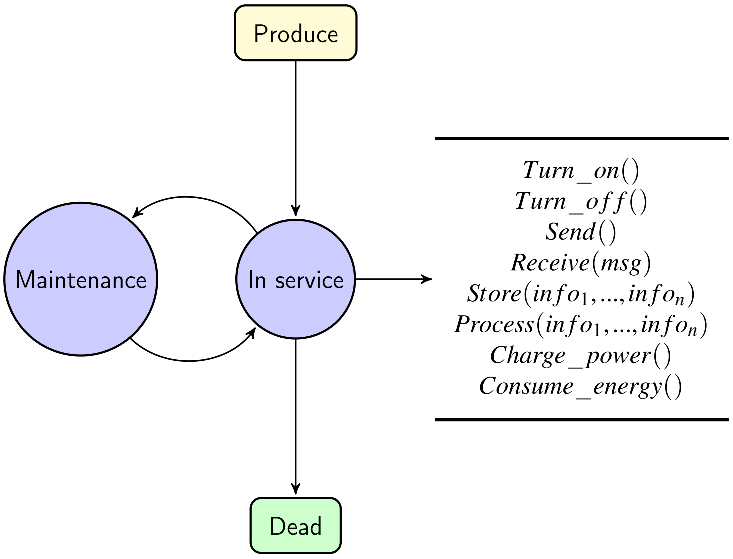


FIGURE 3.15: Cycle life of *Node*.

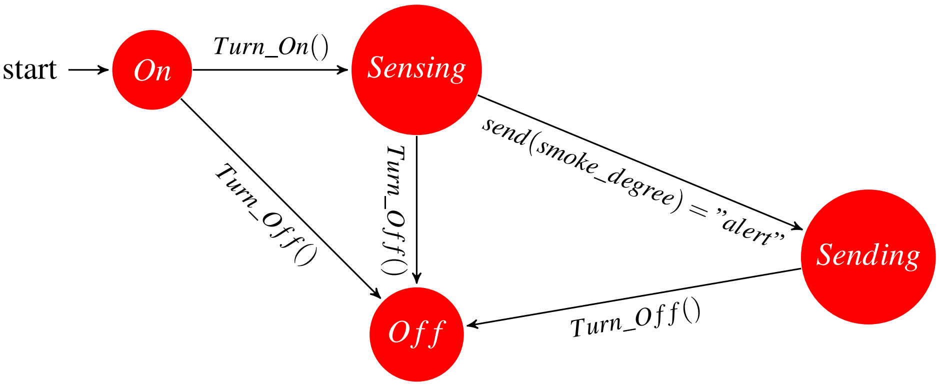


FIGURE 3.16: TA of Sensing/Action fire system.

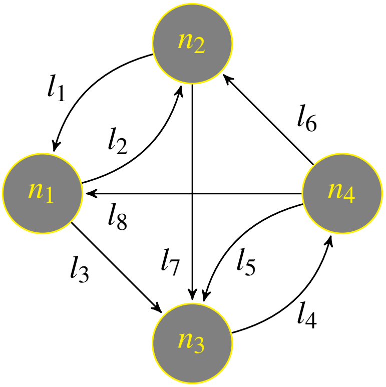


FIGURE 3.17: The connection links of the fire sensors node as a directed graph.

Building obstacles

They are a set of barriers, called "*Obstacles*", which construct the smart city form such as the buildings, roads, markets, homes, etc. The *Obstacles* have a negative *impact* on the propagation of the signal in the air, taking into account its *type* "γ" (wall, wood, glass, etc.), *thickness* "τ", *number* ω, and the *distance* "α" between the two points (transmitter and receiver). The following path-loss models *PL* [**path-loss**] shows how to calculate the value of the signal through the previously mentioned variables

$$\text{PL=PL}_0 + 10n\,log(\alpha) + \sum_{i=1}^{\omega} PL(\gamma,\tau)_i \tag{3.1}$$

Where, PL_0 is the path loss over a distance of one meter, and n is the path-loss exponent that indicates how fast the path loss increases with distance.

3.7.1.2 The Digital Model (DM)

DM is a collection of digital components and rules to guarantee the functional correctness of **ICTs**. The proposed **DM** covers the adopted protocols, services, and security protocols.

Communications protocols

The IoT communication requirements like the low consummation energy, the reliable connectivity, and the security level are related to the selected communications protocols. For each layer, we adopt the appropriate protocol regarding IoT networks requirement as follows.

Data link layer

- IEEE 802.15.4e is suitable for low power communication. It uses time synchronization and channel hopping to enable high reliability, low cost, and meet IoT communications requirements.

- IEEE 802.11 known as WiFi, where, the original version is the IEEE 802.11 wireless medium access standard. Generally, WiFi does not support IoT devices due to it needs to large power consumption. Its version sister IEEE 802.11 AH treats power consummation problem by increasing the sleep time period. It is suitable for constrained devices having a small memory and low processing by defining a short MAC frame of 12 bytes.

- WirelessHART runs on the top of IEEE 802.15.4 PHY and chooses Time Division Multiple Access (TDMA) in its MAC. It is reliable and secure for small devices supporting security mechanisms for end-to-end, per-hop, or peer-to-peer networks, and, it encrypts messages with advanced encryption.
- Z-Wave is a low-energy protocol and suitable for smart structures with communication of about 30 meters. It is used to communicate short messages like controlling temperature, humidity, light, etc.
- Bluetooth Low Energy consumes less power than the classic Bluetooth protocol, while its latency can reach 15 times more than the initial one.
- Zigbee Smart Energy is suitable for a large range of IoT devices like remote controls and healthcare systems. ZigBee supports the constrained devices and symmetric-key exchange, and it is more scalable by using stochastic address assignment.
- LoRaWAN is to reduce the consummation of IoT device energy. It is characterized by the low cost, secure, mobile, and bi-directional communication for IoT applications.

Network Layer

- Routing Protocol for Low-Power and Lossy Networks (RPL) supports different data link protocols such as IEEE 802.15.4, Bluetooth, Low Power WiFi, etc. It creates Destination Oriented Directed Acyclic Graph (DODAG).
- IPv6 over Low power Wireless Personal Area Network (6LoWPAN) encapsulates IPv6 long headers in IEEE802.15.4 small packets, which cannot exceed 128 bytes. It supports different length addresses, low bandwidth, low cost, different topologies, mobility, scalable networks, unreliability and long sleep time.
- IPv6 over Bluetooth Low Energy supports a short-range wireless communication technology that aims at ultra-low power. It is suitable for sensors transmitting data infrequently or peripherals using asynchronous communication.

Table 3.2 compares the mentioned protocols in terms of architecture, message size, security and IP address used.

Criteria	**RPL**	**6LoWPAN**	**IPv6 over Bluetooth Low Energy**
Architecture and network	DODAG	Wireless personal area network (WPAN)	Master / Slave architecture
Message size	5 bytes of compressed IPv6. 4 bytes for ICMP Type. 24 bytes for DIO Base Object. 16 bytes for DODAG Configuration Option	128-byte maximum frame length in IEEE802.15.4	The Logical Link Control and Adaptation Protocol (L2CAP) sublayer in Bluetooth already provides segmentation and reassembly of larger payloads into 27 byte L2CAP packets
Security	RPL network admits three possible security modes: unsecured, preinstalled, and authenticated. Recent implementations aim to securely connect constrained nodes (as IPsec, DTLS, and IEEE 802.15.4 link-layer security)	Depends on the 802.15.4 security sub-layer (by adding both a Message Integrity Code (MIC) and a frame counter to each frame).	Using the Cipher Block Chaining-Message Authentication Code (CCM) algorithm and a 128-bit AES block cipher. 4-byte Message Integrity Check (MIC) is included in the Bluetooth LE packets. Encryption is applied to the PDU payload and MIC fields.
IP address	IPv6	IPv6	IPv6

TABLE 3.2: Comparison between the network layer protocols.

Application Layer

- Message Queue Telemetry Transport (MQTT) is based on a Publish/Subscribe architecture that is composed from three devices: publisher, broker, and the subscriber. The broker is implemented by the set of topics which have an hierarchical form that is divided into multi-level (e.g: Building/room_1/temperature), the subscribers relate these topics, the publisher as the sensors puts its collected information at one topic in the broker. Then, the broker forwards messages to the nodes subscribed in the same topic.

  Its quality of service is covered of three classes: the publisher sends one message and the broker has nothing to do with the acknowledgement of receipt (QoS 0), the publisher re-sends the same data until it receives an acknowledgement message from the subscriber (QoS 1), the acknowledgement process between the sender and the receiver is applied at two levels (QoS 2). MQTT is prepared to be an open source, lightweight, simple and easy to implement, also it supports all platforms and a diverse of popular programming languages.

The sequence diagram in Figure 3.18 illustrates the *connection link* of, the example of a fire case, three main *Nodes* communication through the MQTT protocol: Sensor (senses a measurement as a smoke degree), Broker (subscribe the *Nodes*, receive the messages from the *Nodes* published and send the commands to the *Nodes* subscribed) and Actuator that executes an action (spray the water).

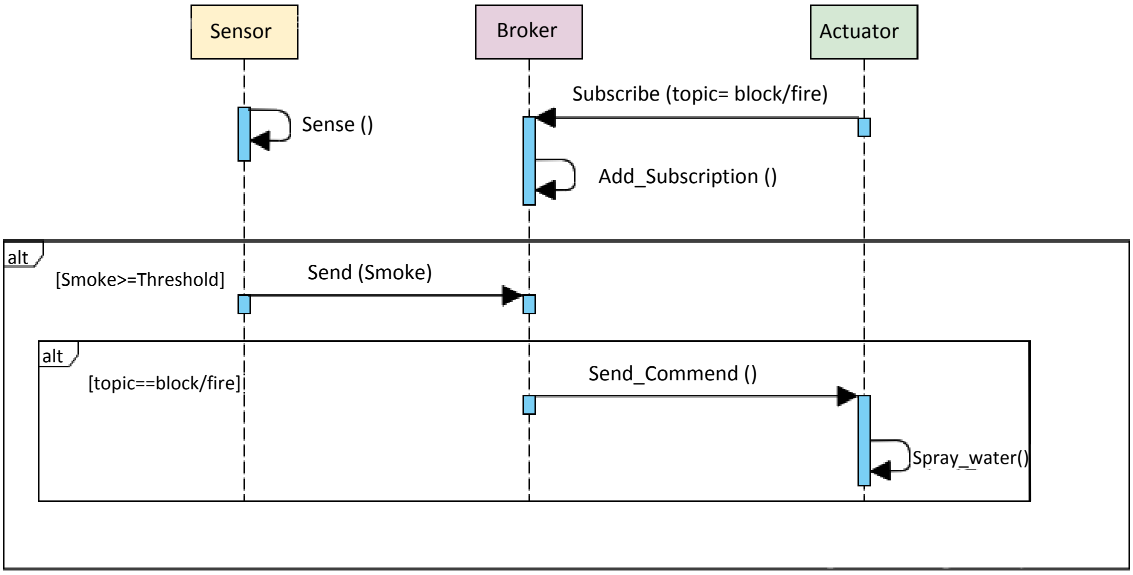
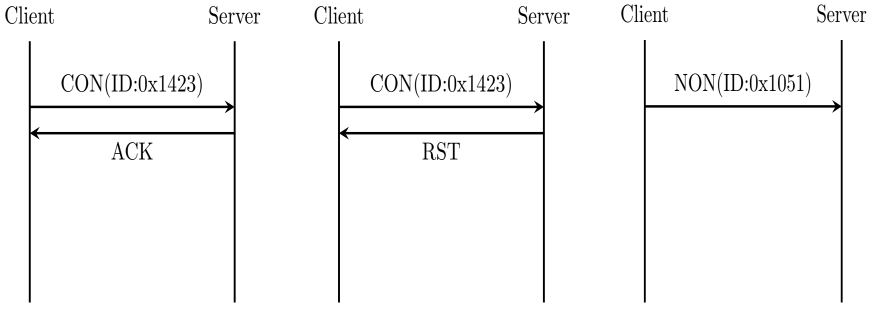


FIGURE 3.18: The sequence diagram of the MQTT protocol.

- The Constrained Application Protocol (CoAP) runs in REST architecture (client/server). The sent message from the client to the server is one of the four RESFful methods (GET, PUT, PUSH and DELETE). It is featured by the low energy consummation, secure by the DTLS protocols [204] that encrypts the data flow, and high latency based on UDP protocol. This protocol has low bandwidth with a loss of information. The end-to-end communication used by this protocol consists of two kind of messages: Confirmable and Non-Confirmable messages. The first is a request sent from the client to the server and requires an acknowledgement from the server, when the server receives this message, it responses by the message ACK, else, it sends rest message (RST) 3.19(a). The Non-Confirmable message does not need an acknowledge by the server 3.19(b). We note that, the Confirmable messages are a critical information whereas the Non-Confirmable can be a measured information published from the sensors to the server.



(a) Confirmable Messages (Reception/Loss). (b) Non-Confirmable Message.

FIGURE 3.19: CoAP processes.

- The Advanced Message Queuing Protocol (AMQP) runs over TCP and based on the publish/ subscribe architecture. The broker is divided into two components: exchange and queues. The exchange receives published messages from the producers and transmits them to queues which send them to the consumers. Four methods are used to transform the message from the exchanges to the queues. Direct, where, the exchange routes the message to the queues that have the binding key equals the routing key of the message (Fig.3.20). Fan-out, where ,the exchange transmits the message to all the queues related with it without constraints. Header, where the message transmitted from the exchange has the pair Key-Value to identify which queue can receive this message. Topic is when the exchange sends the massage to the queues if the queues patterns are identical with the routing key of the message.

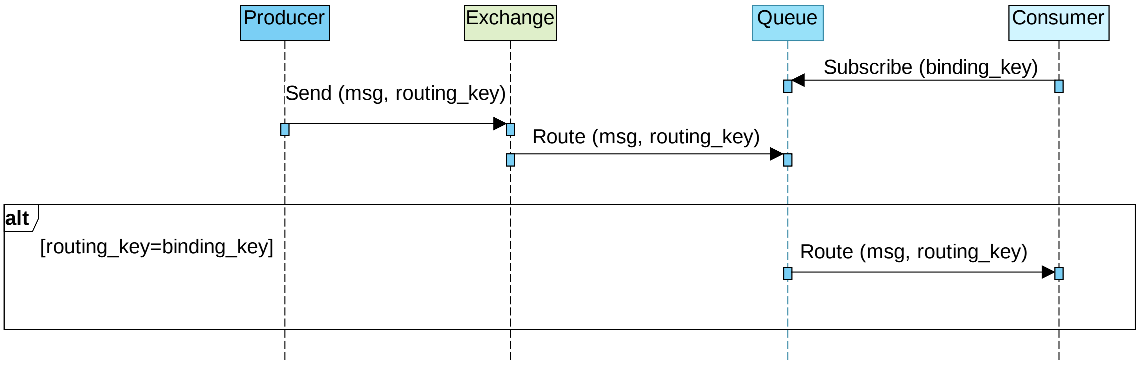


FIGURE 3.20: The operation of AMQP with Direct exchange method.

These messaging protocols differ on message size, power consummation, latency, QoS, security level and the number of M2M usage [205]. CoAP has the lowest message size and overhead compared to MQTT and AMQP. CoAP protocol requires lower power and resources than the MQTT and AMQP protocol. CoAP protocol offers lowest bandwidth and latency than the MQTT and AMQP protocol. MQTT has the highest level of quality of services with the least interoperability between them. AMQP provides the highest level security and additional services, while MQTT supports the lowest level of security and additional services. MQTT is used by many organisations but it does not remain a global standard.

Table 3.3 compares the discussed protocols in terms of architecture, abstraction, header size, message size, communication methods, quality of service, security and communication port.

Criteria	**MQTT**	**CoAP**	**AMQP**
Architecture	Client/Broker	Client/Server or Client/Broker	Client/Broker or Client/Server
Abstraction	Publish/Subscribe	Request/Response or Publish/Subscribe	Publish/Subscribe or Request/Response
Header Size	2 Byte	4 Byte	8 Byte
Message Size	Small and Undefined (up to 256 MB maximum size)	Small and Undefined (normally small to fit in single IP datagram)	Negotiable and Undefined
Semantics/ Methods	Connect, Disconnect, Publish, Subscribe, Unsubscribe, Close	Get, Post, Put, Delete	Consume, Deliver, Publish, Get, Select, Ack, Delete, Nack, Recover, Reject, Open, Close
Quality of Service (QoS)/ Reliability	QoS 0 - At most once (Fire-and-Forget), QoS 1 - At least once, QoS 2 - Exactly once	Confirmable Message (similar to At most once) or Non-confirmable Message (similar to At least once)	Settle Format (similar to At most once) or Unsettle Format (similar to At least once)
Security	TLS/SSL	DTLS, IPSec	TLS/SSL, IPSec, SASL
Default Port	1883/ 8883 (TLS/SSL)	5683 (UDP Port)/ 5684 (DLTS)	5671 (TLS/SSL), 5672

TABLE 3.3: Comparison between the session layer protocols [205].

As example, the sequence diagram in Figure 3.21 illustrates the behavior of the IoT appliances that communicate with the session layer protocols, MQTT in particular. We propose a fire scenario in a smart building equipped by a fire sensor and the actuators to extinguish the fire by spray water. The MQTT broker processes the received message from the fire sensor, then, it sends a command to the actuator to put the fire out, as well as, it sends an alert message to the fire service.

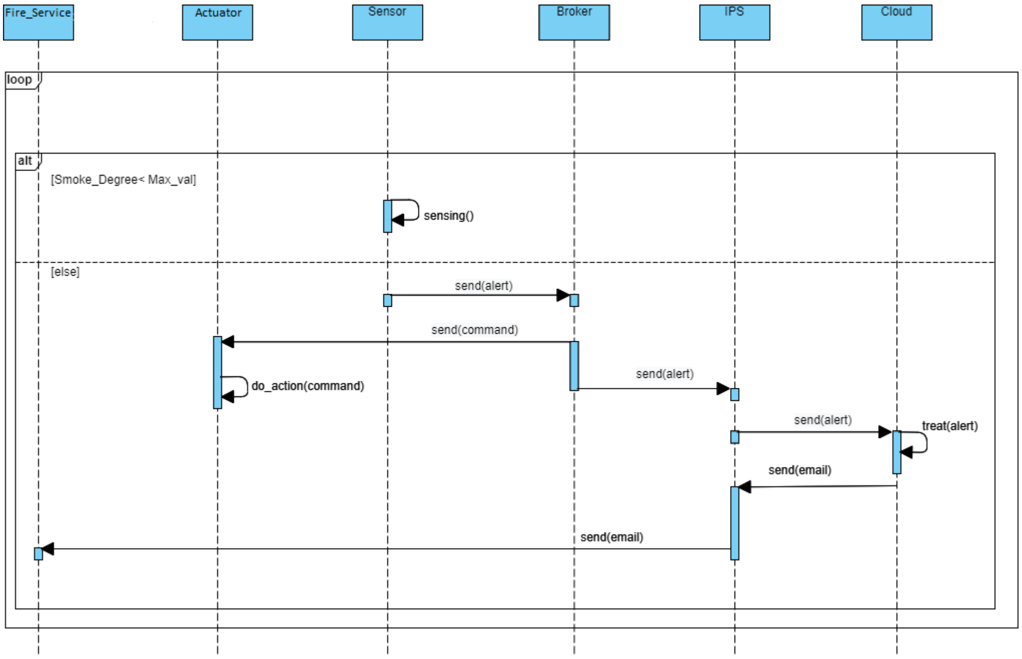


FIGURE 3.21: Fire example in the smart city.

3.7.1.3 Services

The management of a smart city platform needs several decisions to be taken in real-time to improve its QoS. The proposed framework develops the following services.

Security

- Secure sub-architecture: The internal sub-architecture is installed inside the building like the DMZ, the Virtual Local Area Network (VLAN) [206]; while the external sub-architecture is an outdoor network where the routing is based on IP addresses. It links the varieties of internal sub-architecture in one root like the cloud and the fog computing to analyze, store the received data, and manage the IoT networks.

- Secure components: Due to the threats that affect the communication network and operating systems with a direct influence on the information integrity and the availability of services, it has become necessary to distribute a set of protection tools, in all levels of the network. The security components encrypt the transmitted data, make an Access Control Lists (ACL), detect and prevent an intrusion. Among them we deploy firewall [207], VPN [208], IDS [197], IPS [198], Proxy [209], Kerberos Servers [210], and anti-virus [211], etc.

Communication supports

It is an adoption of facilities and materials designed by a low latency, a large coverage area, protection, low-cost (energy consummation, deployment, maintenance cost, etc.). These requirements are granted by considering the following technologies.

- 5G: It is widely used with portable devices, especially mobile phones, and this is due to its high frequencies, which need small pickups to match it. This service solves two IoT requirements: mobility and latency. This service is provided at the *communication level* of the proposed architecture.
- Optical fiber: This technology is deployed to connect remote points with high flow. It guarantees reliability and speed at the *communication level* of the architecture.
- Computing and storage layer: At the *processing and storage level*, it is configured to receive and process high flows, as the quality of service is related to their capabilities (processing, storage, protection, service presence, etc.).

Maintenance

The availability of services is one of the most important requirements in a smart city. In this paper, we consider the life-time of IoT nodes and the good functioning of the system. To Avoiding breakdown of the service, we monitor the availability of the IoT devices and analyze the periodic reports in each sub-architecture. These actions allow the network to view the system functioning and predict the IoT problems, e.g., SQL log files records the applied operations and the states of the IoT devices. The file are analyzed by cloud applications as Apache^{TM} Hadoop and Apache Spark^{TM} [212].

Security Policies

To reinforce security in **SCM**, we propose Access Control Models **ACM** as a set of rules and decisions that categorize the responsibilities of the system components and attributes the authorization or prevention access to the components or resources.

ACM is defined by the tuple $\mathbb{M} = \langle\ Subjets, Nodes, Actions, Permissions, Security, Grant\rangle$, where:

- *Subjets* is a finite set of subjects that can execute actions in **SMC**.
- *Nodes* are all physical and digital objects and resources defined by **SMC**.
- *Actions* are all actions that can be executed by *Subjets* and *Nodes*.
- *Permissions*= $\{Read\_down, Write\_up, Access\}$ is a set of restrictions to be granted to the set of *subjects* and *nodes*.
- *Security*:$Subjects \cup Nodes \rightarrow Values$ is an assignment function that attributes a bounded value representing the security level of a subject or an object.
- *Grant*:$(Subjects \cup Nodes) \times Actions \times (Subjects \cup Nodes) \rightarrow 2^{Permissions}$ is a function that manages the execution of actions between nodes and subjects in **SMC**.

Algorithm 2 implements **ACM** in **SCM** where the set of permissions is defined as follows. In addition, the **ACM** processes are shown in the Figure 3.22.

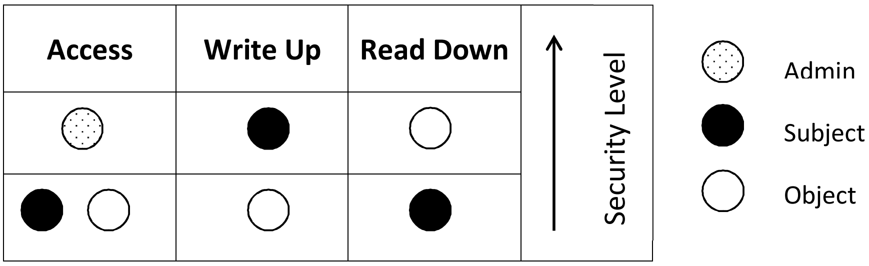


FIGURE 3.22: ACM processes.

- ***read down*** allows the owner to access to the second node without updating its state. The action can be applied if the subject has a security level smaller than the the security level of the node.

- ***Write up*** allows the first node to update the state of the second node (e.g: add, update or delete information). The action can be applied if the subject has a security level greater than the the security level of the node.

- ***access*** is provided only to the *Admin* of the network. This property sets the degree of the security level of another *Non – Admin* or *Node*.

Algorithm 2: Access Control Management

```
/* Case -1-: Read Action */
if $Action == Read$ then
        // o: object, s: subject, $\omega$ is the security level of the admin.
    if $(s.security < o.security) Or (s.security == \omega)$ then
        return $(true)$
    else
        return $(false)$
    end
else
    /* Case -2-: Write Action */
    if $Action == Write$ then
        if $(s.security > o.security) Or (s.security == \omega)$ then
            return $(true)$
        else
            return $(false)$
        end
    else
        /* Case -3-: Access Action */
                // n: is an object or subject, $\iota$: new level inserted
        if $s.security == \omega$ then
            $n.security = \iota$
            return $(true)$
        else
            return $(false)$
        end
    end
end
```

3.7.2 Smart City Analysis

To ensure the correctness and security of the proposed architecture, we rely on UPPAAL model checker for the formal verification and Cooja networking analyzer for simulation.

3.7.2.1 Formal Verification

Uppaal is suitable for our work, in addition to that it is distinguished by several advantages over other model checkers, including:

1. UPPAAL is better for verifying real-time systems (Fig. 3.4) [213].
2. state description for the next location is regarded as an update for parameters in PROMELA, which is not as obvious and specific as an update for parameters in UPPAAL and NuSMV [213].
3. UPPAAL achieves the best performance for timed and non-timed models [214].
4. The results reveal that UPPAAL is more flexible in terms of usability and easiness compared to PRISM [215].
5. Both translating to Promela and μCRL can be difficult under some circumstances, but translating to Uppaal on the other hand never gets really difficult in our case. These results tell us that, at least concerning the turntable model, Uppaal is the best choice when selecting a language based on the difficulty to translate into this language [216] (see table 3.5).
6. A summary of the experienced times when evaluating the property that for all possible executions all the trains eventually complete their missions might still be a useful approximate indication of the impact of a certain system design approach / formal verification technique in terms of performance (Fig. 3.6) [217].

	SPIN	UPPAAL	NuSMV
Safety	established	established	established
No deadlock	established	established	established
Activity	established	established	established
Reachability	established	established	established
Real-tirme	cannot be described	established	cannot be described
Fault tolerance	not established	not established	not established
Concurrency	not established	cannot be described	not established

TABLE 3.4: Comparison of properties verification [213]

- 0: Impossible. Due to differences between the two modeling languages or the limitations of the temporal logic it is impossible to do this.

- 1: Difficult. the translation is not straightforward but can be done using special techniques.

- 2: Needs some work. The translation is not completely straightforward, but it does not require special techniques.

- 3: Easy. Translation or verification can be done easily.

	Assignments	Delays	Guards	Nested parallelism	Shared variables
PROMELA	3	2	1	1	3
μCRL	2	1	3	2	1
UPPAAL t.a.	3	3	3	2	3

TABLE 3.5: Comparison of translation problems [216]

Framework	Range of evalution times
UMC	38 – 86 seconds
SPIN	13 – 47 seconds
NuSMV/nuXMV	2.9 – 43 seconds
CADP	29 seconds
UPPAAL	16 seconds
TLA+	3 minutes
ProB	32 minutes
mCRL2	2 minutes –19 minutes
FDR4	15 seconds –20 minutes
CPN	unable to deal with the state-space size

TABLE 3.6: Indicative Summary of Evaluation Times [217]

It is a modeling and verification tool, Uppaal allows to model the behavior of the IoT network nodes using timed automata formalism. The automata of a node is modeled to exchange the commands with another. To check the security and the correctness of the proposed network, we express the requirements on TCTL input language. It is based on two formulae types, path and state, the state formulae presents one state whereas the path formulae describes the execution of the constructed network. Path formulae has three types reachability, safety and liveness as presented in Figure 3.23 and described as follows.

- **Reachability**: There is a possibility to reach the state satisfying the state property p (E<> p).
- **Safety**: p is correct in all states (A[] p), or there is a path where p is true (E[] p).
- **Liveness**: p is correct in some states (A<> p), or if p is true, q is also true in all the paths (p –> q).

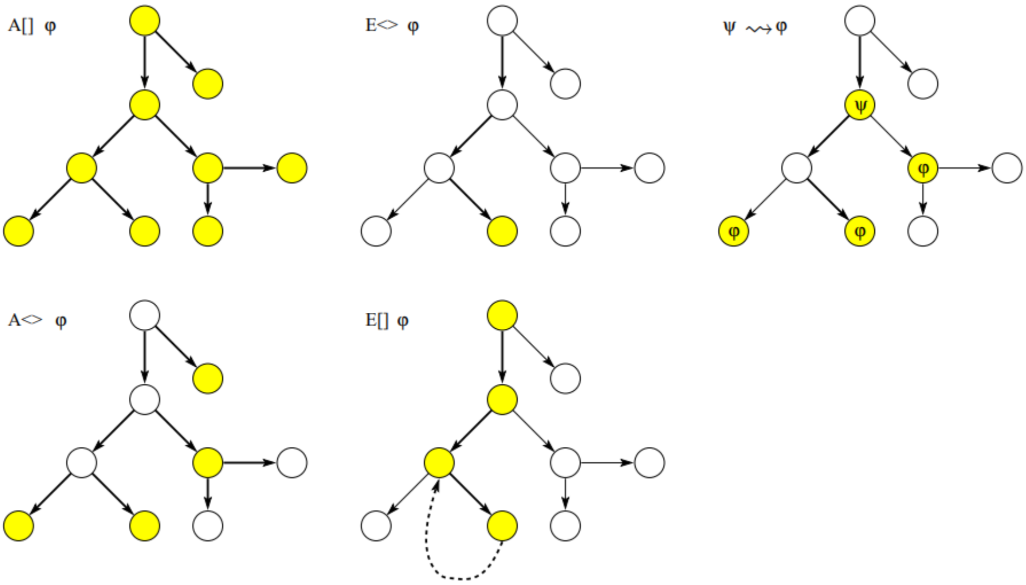


FIGURE 3.23: TCTL Path formulae semantics [193].

3.7.2.2 Network Analysis

Contiki is an open source OS, which is developed to study the behaviors of the WSNs nodes in the IoT networks through Cooja simulator [218] that provides — besides a GUI— the simulation of the radio medium. Its visualisation presents the propagation of the signal produced by the WSNs placed on the area of interest respecting the diffraction, refraction and reflection phenomena. Cooja simulator offers many radio medium types such as Unit Disk Graph Medium (UDGM), Directed Graph Radio Medium (DGRM), Multi-path Ray-tracer Medium (MRM), and others.

The simulation creates a wide environment to simulate the wireless networks through the integration of many types of predefined motes for example Sky motes, ESB mote, micaZ mote, etc. Also, it supports 6LoWPAN, CoAP and RPL protocols, and it gives to the network developers the access to update these packages and to optimize the security, mobility, latency, cost, and all the other IoT requirements. Based on the comparison presented in Tables 3.7 and 3.8, many features have been identified to choose Cooja as a network simulator. Indeed, it supports the concepts that are included in our proposition especially: the multi-path ray-tracing, the obstacles attenuation, constructs direct graph, TCP/UDP protocols, and energy consummation model. Table 3.7 shows the reason for choosing the Cooja simulator among the other network simulators.

3.8 Experimental Results

This section shows the effectiveness of our developed framework, in which validity and robustness of the proposed **SCM** are verified through experiments by applying verification and simulation techniques. First, we prepare our **SCM** model. Then, we use Cooja simulator to show the effect of IoT protocols on the consummation of energy for the constrained devices as well as the impact of the obstacles on the communication among the nodes to increase the network lifetime. Finally, we check the correctness of the **SCM** on Uppaal with respect on the functional, the behavior of the devices subject to the security policies is also studied.

3.8.1 SCM description

The area presented in Figure 3.24 has eight heterogeneous buildings that are divided into homes of $(10 \times 10m^2)$. Each building has a *sink* node to collect the temperature measures sent by *sensors*. The deployment of sensors are arbitrary distributed.

Figure 3.25 shows the architecture of our concrete **SCM** that we want to analyze. It is a client/server architecture based on RPL, CoAP, and MQTT protocols. The third level represented by the processing unit (as in Figure 3.13) is equipped by the cloud computing server that records less-used information (e.g, buildings status report per week) and the fog computing service which stores frequently the most used information (e.g, the measured data). Further, it has the ISP that supports the wire and wireless communication. In this architecture, we consider unconstrained and constrained devices; the unconstrained devices are the communication, filtering, routing and protecting appliances (computers, firewall, routers and the IDSs respectively). The constrained

Simulator	ns2	Castalia OMNet++	TOSSIM	Cooja/MPSim	WSim/WSNet
Level of details	generic	generic	code level	all levels	all levels
Timing	discrete event	discrete event	discrete event	discrete even	discrete event
Simulator platforms	FreeBSD, Linux, SunOS, Solaris, Windows (Cygwin)	Linux, Unix, Windows (Cygwin)	Linux, Windows (Cygwin)	Linux	Linux, Windows (Cygwin)
WSN platforms	n/a	n/a	MicaZ	Tmote Sky, ESB, MicaZ	MicaZ, Mica2, TelosB, CSEM Wisenode, ICL BSN nodes, eZ430
GUI support	Monitoring of simulation flow	Monitoring of simulation flow, c++ development, topology definition, result analysis, and visualization	None	Yes	None
Wireless channel	Free space, two-ray ground refection, shadowing	lognormal shadowing, experimentally measured, path loss map, packet reception rates map, temporal variation, unit disk	lognormal shadowing	multipath ray-tracing with support for attenuating for obstacles, unit disk, directed graph	file static, disk model, free space, tworay ground, lognormal shadowing, rayleigh fading, ITU indoor model, nakagami fading
PHY	Lucent WaveLan DSSS	CC1100, CC2420	CC2420	CC2420, TR1001	CC1100, CC1101,CC2500, CC2420
MAC	802.11, preambule based TDMA (preliminary stage)	TMAC, SMAC, Tunable MAC (can approximate BMAC, LPL, etc.)	Standard TinyOS 2.0 CC2420 stack	CSMA/CA, TDMA, XMAC, LPP, NullMAC, contikiMAC, SicslowMAC	DCF, BMAC, ideal MAC
Network	DSDV, DSR, TORA, AODV	Simple Tree, Multipath Rings	No data	RPL, AODV	Greedy Geographic, file static
Transport	UDP, TCP	None	No data	UDP, TCP	None
Sensing	Random process with Mannasim add-on	Generic moving time-varying physical process	No data	Moving nodes	Generic moving time-varying physical process
Energy consumption model	Yes	Yes	With Power TOSSIM add-on	Yes	Yes

TABLE 3.7: Open-Source Simulators Comparison [219].

Features	Symphony	TOSSIM	Cooja	FreeRTOS	ns-3
Uses real code base	Yes	Yes	Yes	To some extent	no
eserves OS execution model	Yes	Yes	Yes	Yes	-
Enables real-time simulation	Yes	No	Yes	No	Yes
Hardware emulation	Yes, via models	No	Limited	No	Yes, via model
Accounts for hardware-induced delays	Yes	No	To some extent	No	No
Incorporates energy models	Yes	Yes	Yes	No	Yes
Accounts for clock skew	Yes	No	No	No	No
Can accommodate multiple applications	Yes	No	Yes	No	Yes
Can be used with multiple OS	Yes	No	Yes	No	-
Customizable simulation detail	Yes	No	Yes	No	-
Realistic sensor data feed	Yes	No	No	No	No
Scalability	Limited by hardware	20,000 nodes	$<$ 20,000 nodes	-	350,000 nodes
Up to date OS	Yes	Yes	Yes	Last updated in 2010	-

TABLE 3.8: A comparison of the functionality provided by selected network simulators [220]

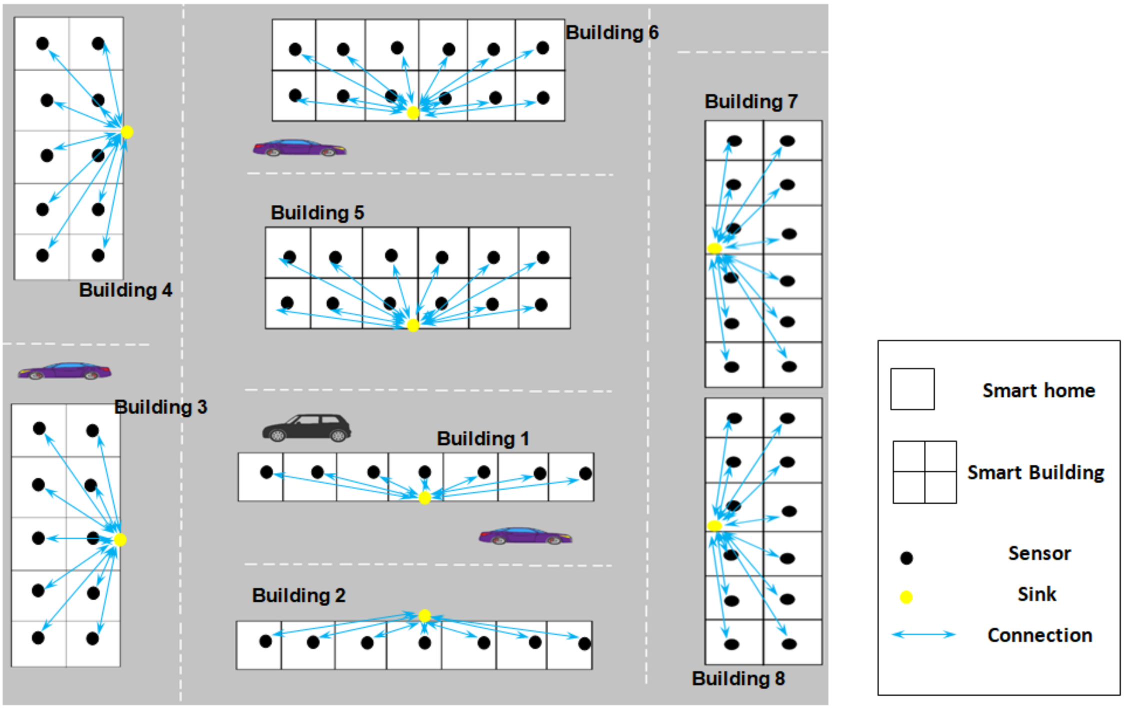


FIGURE 3.24: Area of interest: Set of a Smart Building

devices play the role of the fire detection system (fire sensor, broker, and an actuator that spray the water into the emergency case). The fire system nodes communicate through MQTT protocol.

3.8.2 Cooja simulation

With this test, all the BIM sensors use RPL protocols to transmit the temperature measured in the buildings. The Multi-path Ray-tracer Medium (MRM) model is an extension chosen to simulate the presence of obstacles.

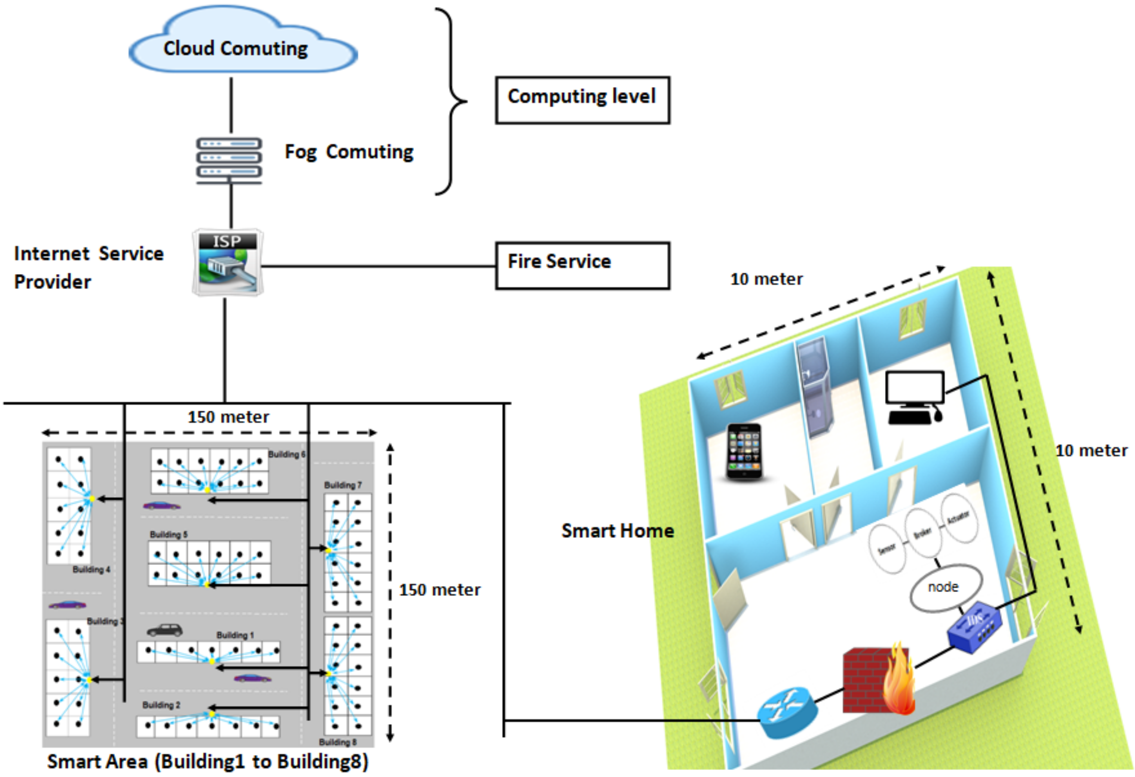


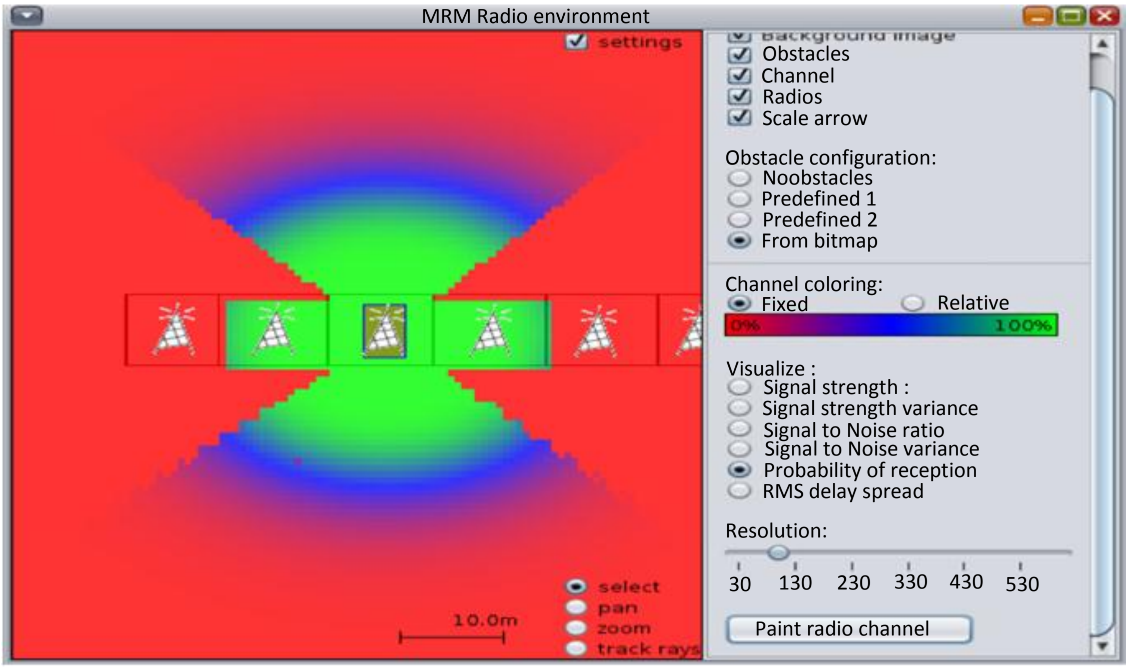
FIGURE 3.25: Area of interest: Smart City.

Table 3.9 shows the used parameters in MRM simulation that takes into account the refraction, reflection, and diffraction phenomena which affect the trend of the transmitted signals. By following the proposed architecture guidelines that avoid constructing the global network which helps to reduce the resources use of Contiki OS computer container. We divide the global network into multi sub-networks related by sinks. Then, the RPL protocol constructs a graph of routes (DODAG) using MRHOF algorithm, we chose this algorithm instead OF0 algorithm due to MRHOF is more reliable, because, in busy simulations, where, many nodes contain a high rate of data, MRHOF would reduce "Packet Drop Ratio" by 25.1% [221].

Parameter	**Value**
Default transmitter output power	1.5 dBm
Receiver sensitivity	-100 dBm
Refraction coefficient	-3 db
Reflection coefficient	-5 db
Diffraction coefficient	-10 db
Obstacle attenuation	-3 db/m

TABLE 3.9: MRM Simulation Parameters.

Figure 3.26 illustrates the probability of receiving the signal of one sensor in the area of interest (sensor 3, building 1, Figure 3.24), where the type of color (green, blue and red) determines the percentage of reception (strong, medium and week respectively). It is clear that the obstacles stop or decrease the signal propagation among nodes.



MRM Radio environment

☑ settings

☑ Background image
☑ Obstacles
☑ Channel
☑ Radios
☑ Scale arrow

Obstacle configuration:
○ Noobstacles
○ Predefined 1
○ Predefined 2
● From bitmap

Channel coloring:
● Fixed ○ Relative

Visualize :
○ Signal strength :
○ Signal strength variance
○ Signal to Noise ratio
○ Signal to Noise variance
● Probability of reception
○ RMS delay spread

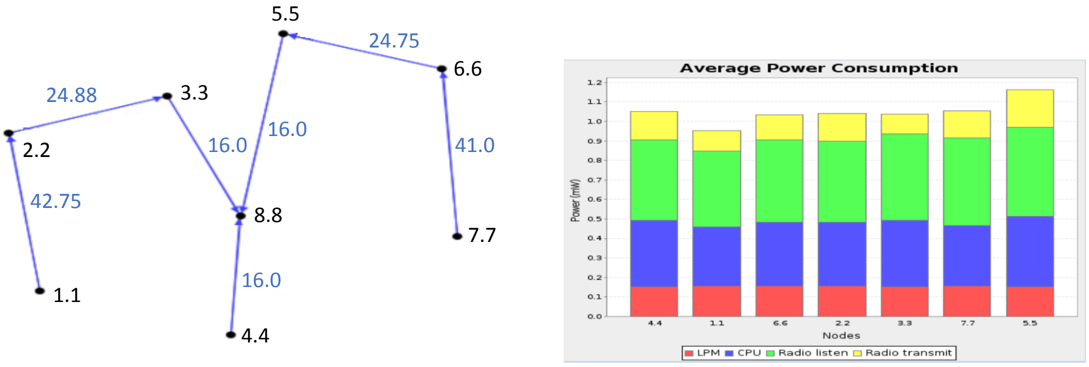
Resolution:

● select
○ pan
○ zoom
○ track rays

FIGURE 3.26: Probability of receiving signals.

From the simulation results, we found that any WSN recognizes its neighbours to construct the DODAG. During 5 minutes of simulation, the nodes in each building constructs its DODAG, where the sink is the meeting point of all orientations. We observe that all WSNs are presented and connected to transmit the collected data to the sink. DODAG edges are weighted to represent the connectivity quality between nodes affected by the distance and obstacles. Figures 3.27(a), 3.28(a), 3.29(a), 3.30(a), 3.31(a), 3.32(a), 3.33(a) and 3.34(a) are DODAGs for the buildings 1,$\cdots$, 8. If the value of a DODAG edge is high, it means that the possibility of receiving data between nodes connected by such edge is low. For example, $node_1$ represented in the DODAG of Figure 3.27(a), located in the first home of the Building 1, is far from the *sink* ($node8$) and its wireless communication passes through many obstacles. Thus, it has the greatest value (42) compared to others.

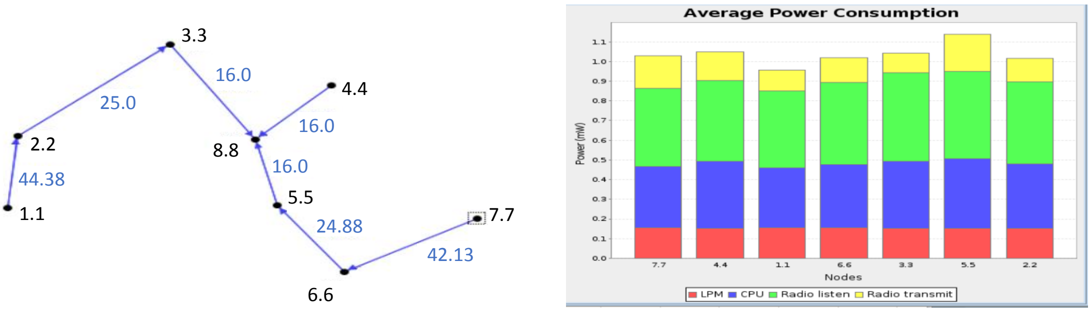
After the connectivity insurance, we analyze the energy consumption of nodes in each building. Figures 3.27(b), 3.28(b), 3.29(b), 3.30(b), 3.31(b), 3.32(b), 3.33(b), and 3.34(b) illustrate the



(a) DODAG.

(b) Consummation of energy.

FIGURE 3.27: Results in building 1.

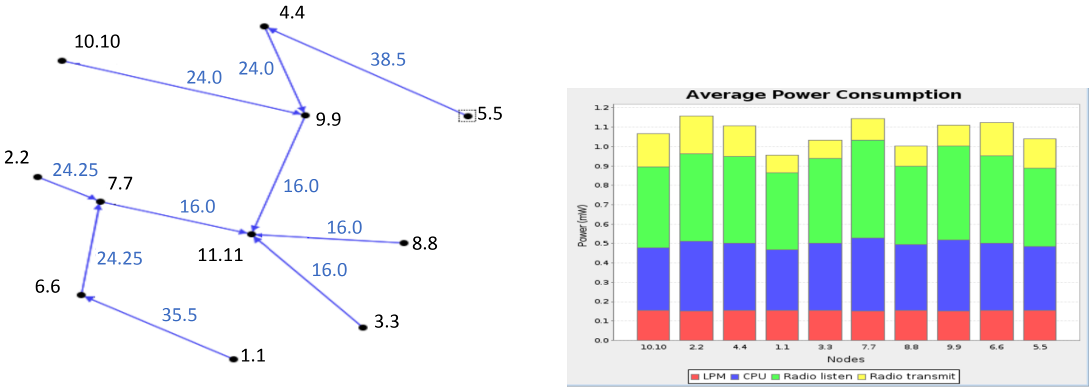


(a) DODAG.

(b) Energy Consumption.

FIGURE 3.28: Results in building 2.

energy consumed in all buildings nodes concerning the number of executed operations: sensing by using LPM (red color), processing by using a CPU (blue color), receiving using a radio listener (green color), and sending by using a radio transmitter (yellow color).

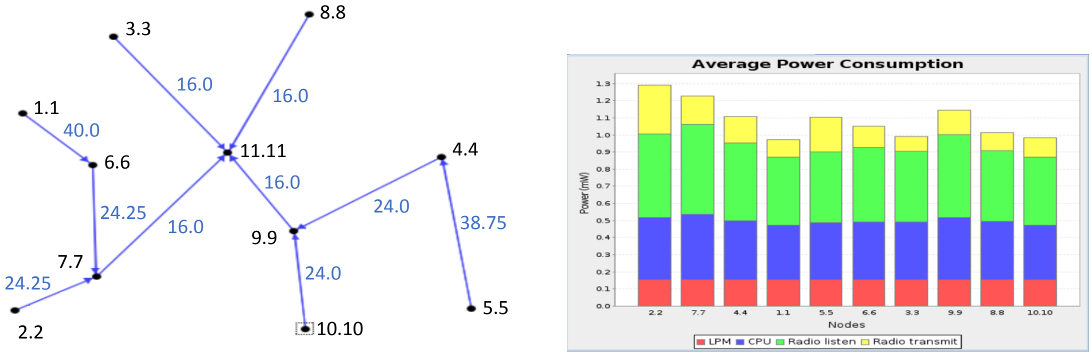


(a) DODAG.

(b) Consummation of energy.

FIGURE 3.29: Results in building 3.

For example, Figure 3.27(b) represents the consummation of energy of the sub-network which its DODAG is represented in the Figure 3.27(a). We observe that the node five has a huge consummation of energy compared to the other nodes due to its position, where, it plays the mediation role between the sink (node eight) and other distant nodes (six and seven). Thus, the node five executes many operations (receive, send, forward, process) to assure the transmission among the sink, itself and the distant nodes.

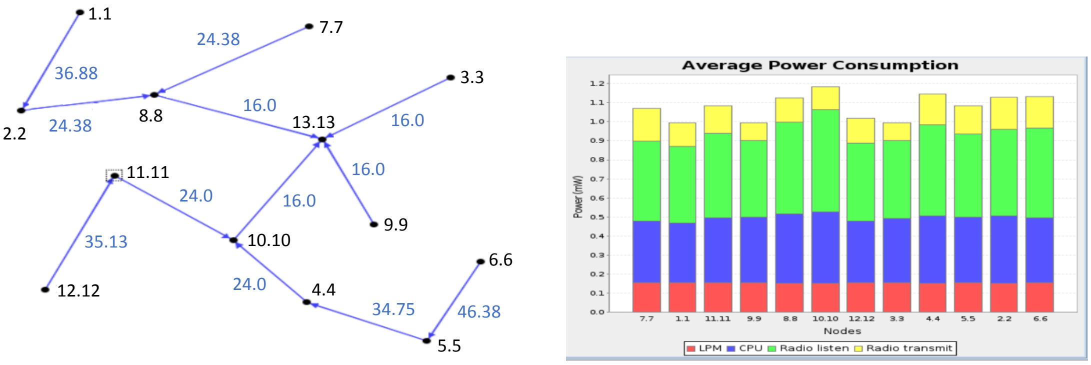


(a) DODAG.

(b) Consummation of energy.

FIGURE 3.30: Results in building 4.

We observe that the most of nodes consume the same level of energy regarding sensing operation while their energy consumption differs when processing, sending and receiving data.



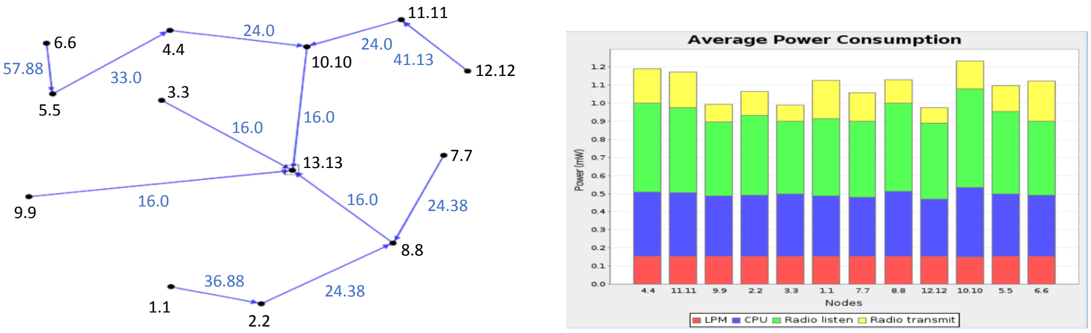
(a) DODAG.

(b) Consummation of energy.

FIGURE 3.31: Results in building 5.

Finally, Table 3.10 compares the energy consumption of the deployed IoT nodes to some homes appliances [222]. The comparison shows that the IoT networks have more lifetime than other type of networks. At Cooja simulation, we assure that:

- Constrained devices are characterized by a low consummation of energy and, the use of RPL protocol can reduce the cost of the IoT network, and increase its lifetime.



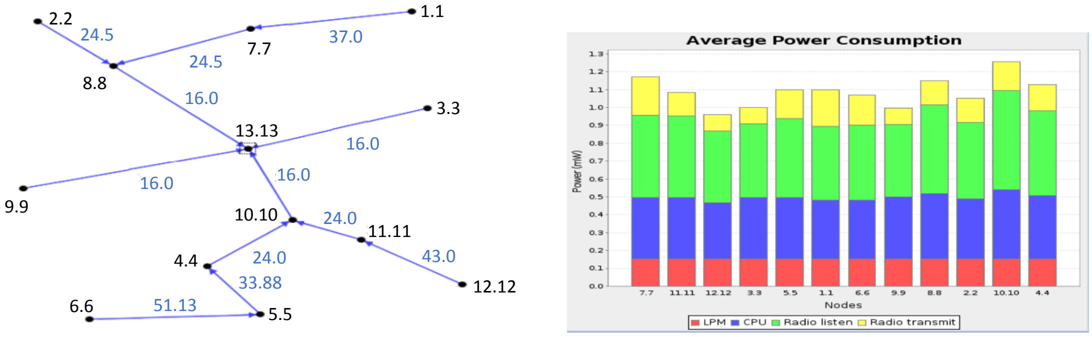
(a) DODAG.

(b) Consummation of energy.

FIGURE 3.32: Results in building 6.

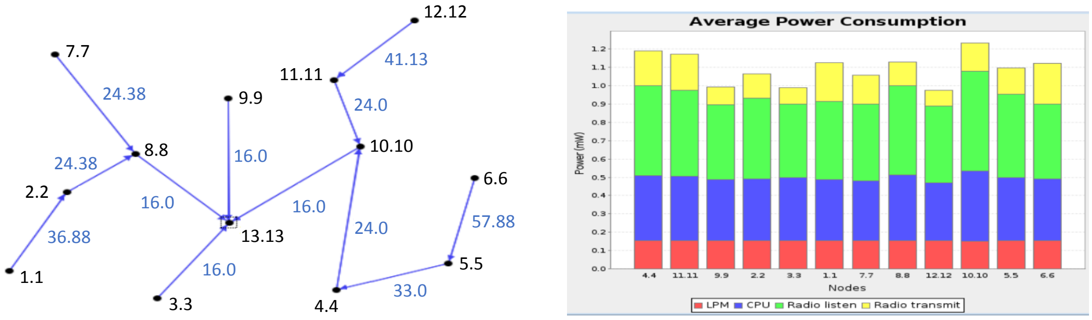
- Dividing the first level of the architecture (Figure 3.13) into multi sub-network decreases the load of operations applied to the sink node due to its low processing capacity and memory storage.

- The obstacles heavily impact the transmission of the signal that causes low QoS. This issue motivates the integration of a new mechanism that finds the optimal positions for WSNs.



(a) DODAG. (b) Consummation of energy.

FIGURE 3.33: Results in building 7.



(a) DODAG. (b) Consummation of energy.

FIGURE 3.34: Results in building 8.

Device	Wattage
IoT simulation node	0.00114
Desktop computer	6.25
Ceiling fan	2.92
Video game system	3
LED TV	6.58

TABLE 3.10: The parameters used in the MRM simulation.

3.8.3 Uppaal Verification

As a second step, by using Uppaal we check the correctness and the security of the modeled **SCM** (Figure 3.25). First, we construct the automata of all **SCM** components which are: sensor, actuator, navigator, IDS, firewall, router, ISP, Fog and cloud service. Figure 3.35 depicts each component semantics by representing their behaviors, including: actions, states, and attributes. Then, we run and verify four possible scenarios.

Scenario 1. The first scenario checks the RESTful Web services used by the CoAP based on

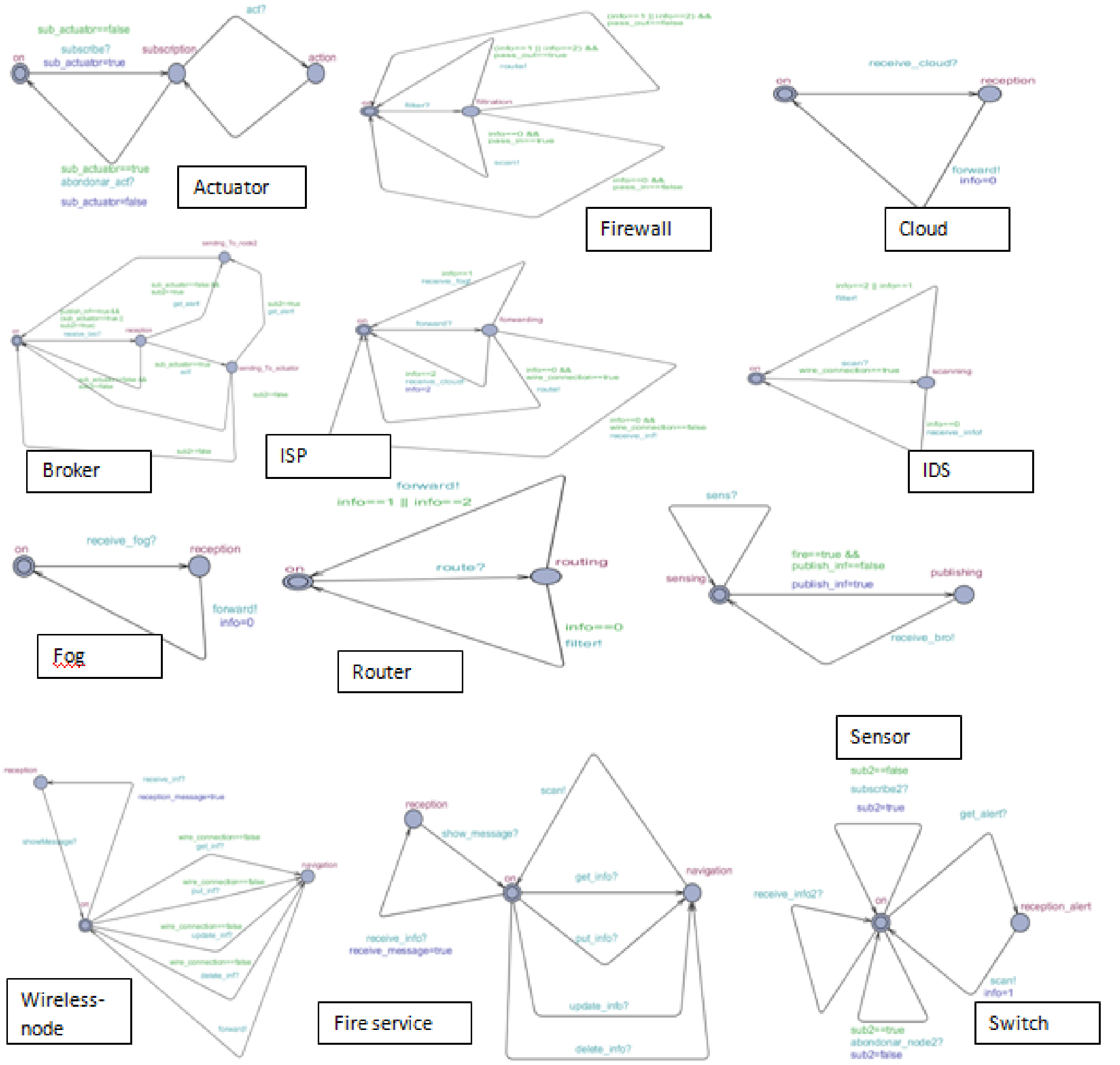


FIGURE 3.35: Timed automata of smart city devices.

the client-server architecture, and consists on the methods: GET, PUT, PUSH and DELETE. The building computer sends a GET request to the cloud service to access the data stored in cloud. The request traverses the three levels of architecture, and any node receiving the request will forward it to the following node. The progress of the behaviour nodes is represented in the sequence diagram showed in Figure 3.36.

Scenario 2. This scenario is similar to the first one, while, it uses the wireless communication protocol to access to the fog service. The sequence diagram in Figure 3.37 shows the progress steps in this wireless navigation.

Scenario 3. The third scenario aims to monitor the fire alarm system and to analyze the fire

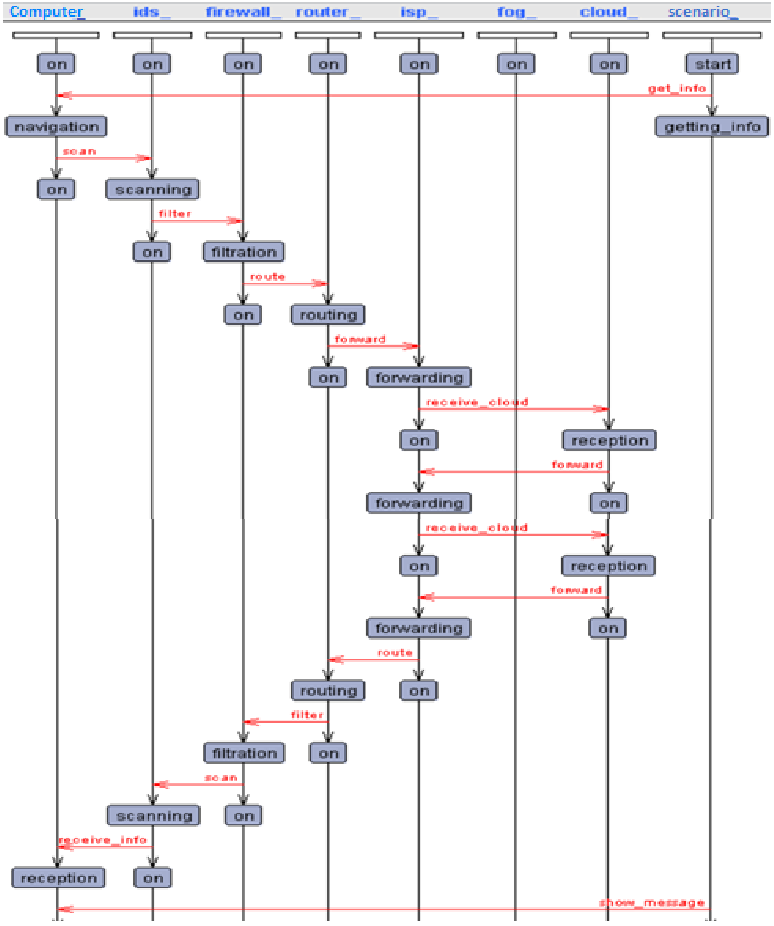


FIGURE 3.36: Sequence diagram of scenario 1.

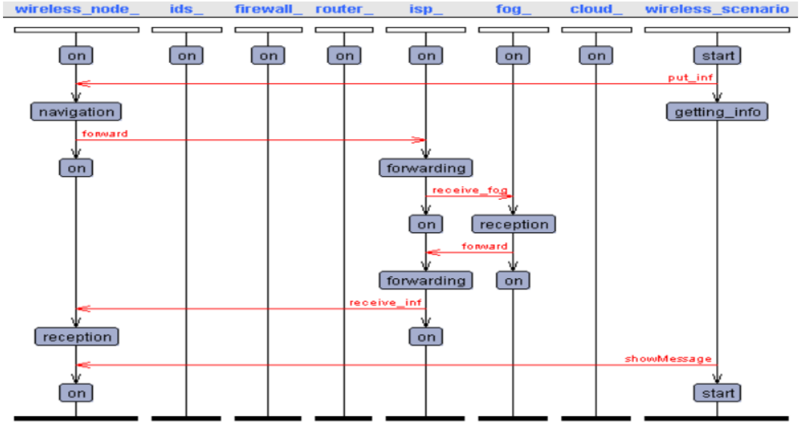


FIGURE 3.37: Sequence diagram of scenario 2.

case resulting in smart buildings and also to check the reaction of the IoT nodes in the network. The global architecture consists of two sub-architectures, client/broker architecture (which has a sensor, broker, and actuator) and declaration architecture (which has bridge and fire service), all the latter are the main components in architectures, but they have the ability to expand. The sensor monitors and sends an alarm to the broker in the fire case, the broker sends the command (stop the fire) to the actuator that is subscribed on it, and the subscribed actuator in the broker receives the command from it. We relate the broker by another node (bridge) to inform the fire service (e.g., message describing the location of the building and the time of the incident). The sequence diagram presented in Figure 3.38 illustrates the steps of this scenario.

Scenario 4. In this scenario, we test our proposed access control model, where, we model three automata: $Admin$, $Subject$ and $Node$. The role of $Admin$ is to set the security level in $Subject$ and $Object$, the $Subject$ randomly can be $Admin$ or $Non-Admin$. The $Subject$ applies actions to $Object$ according to the security level of the $Subject$ and $Object$. All security properties (**read, write and access**) are respected according to the alternative security level of the components presented in Figure 3.39.

Verification. By expressing the security and functional requirements in TCTL, Table 3.11 describes the list of the requirements to be valid without access control, whereas, Table 3.12 lists the set of properties proper to the access control. The verification results show that all the properties are satisfied which means that the architecture is correct and secure concerning the specified requirements.

3.9 Conclusion

In this chapter, we represented the behaviors, the characteristics, and the actions of the effective nodes distributed in the buildings through the formal methods, timed automata, and sequences diagrams. In addition, we suggested a hybrid technique that merges two different concepts which are the modeling and the network analysis. In the next step, we automatically deploy smart components of an area of interest in the smart city.

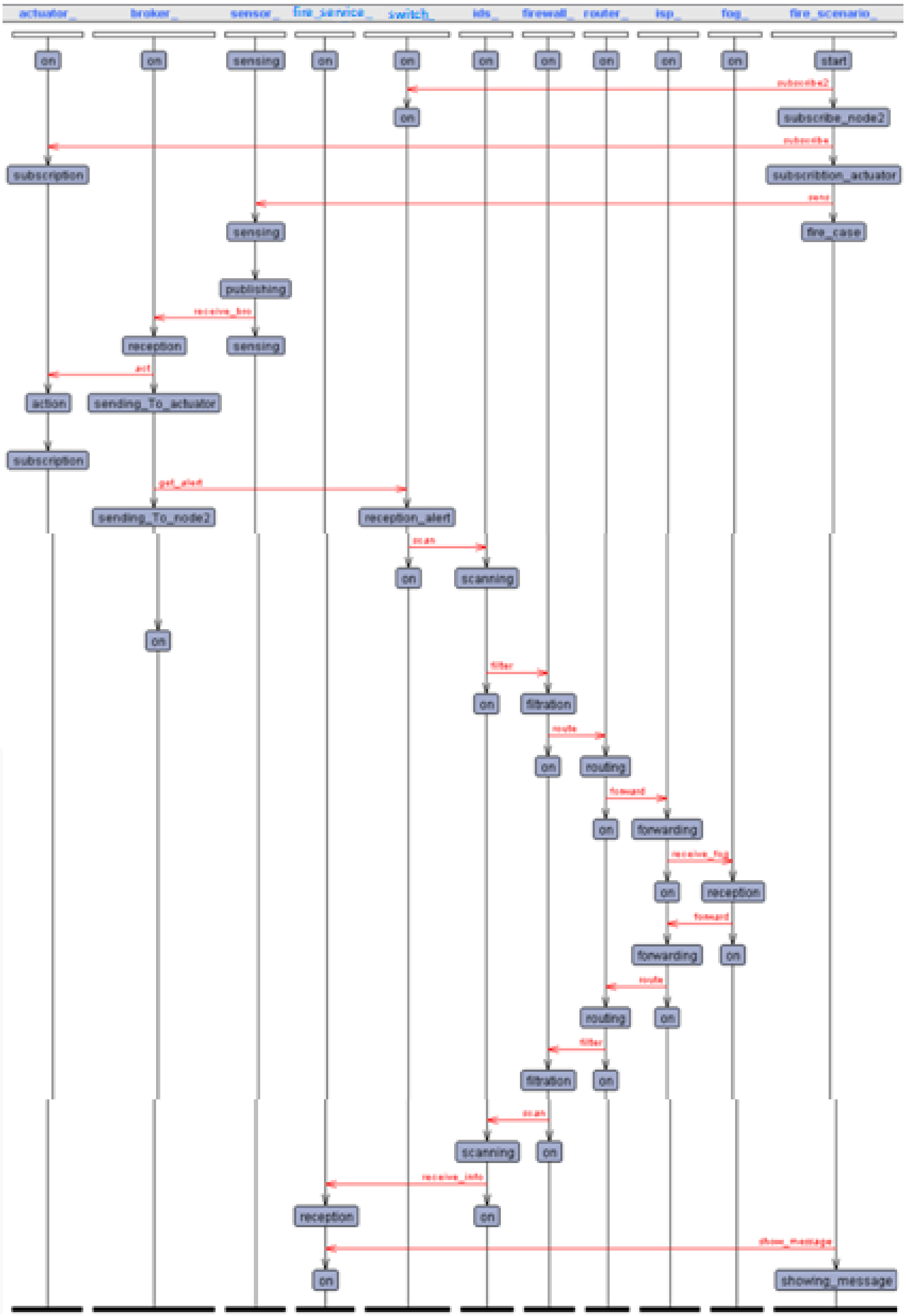


FIGURE 3.38: Sequence diagram of scenario 3.

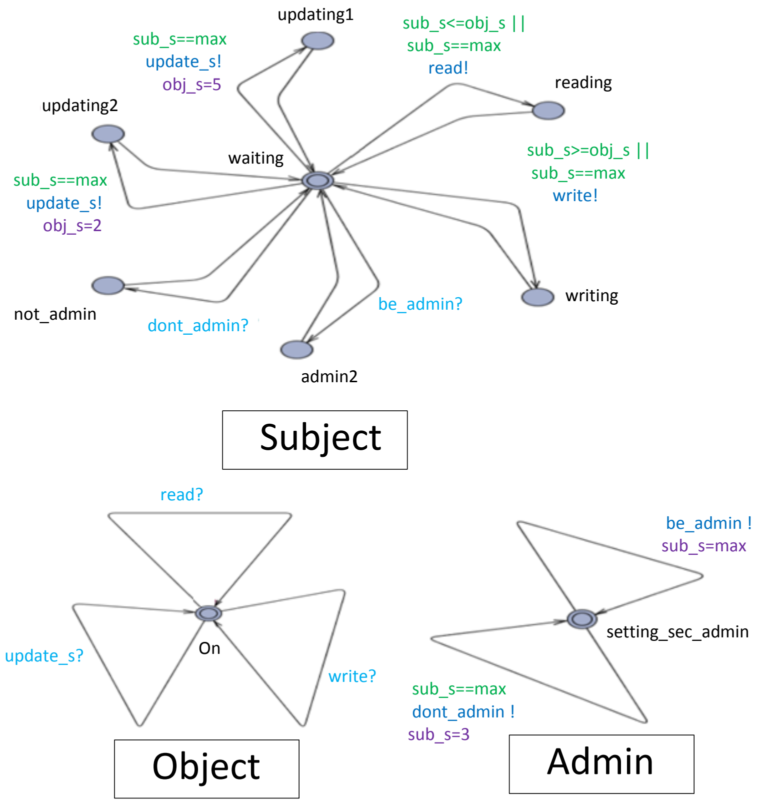


FIGURE 3.39: TA of ACM scenario.

TCTL proprieties	Description
A[] not deadlock	All nodes run without deadlock.
A[] not(ids_.scanning) and not(firewall_.filtration) and not(router_.routing) imply wire_connection==false	We cannot use the wire devices if the type of connection is wireless.
A[] sub2 == false imply not(fog_.reception)	If a node send the alert message that is not subscribed in the broker, then the fog service cannot receive the alert.
A[] sensor_.publishing imply (fire==true)	The sensor can publish in the broker only when it senses a fire case.
A[] node_.reception imply fire == true	The distant node like the fire service can receive alert message in the fire case.
A[] actuator_.action imply (fire==true and sub_actuator==true)	The actuator applies an action (e.g, spray water) when it subscribes in the broker and in the fire case.
A[] fog_.reception imply info==1 and pass_out==true and ware_connection==true	The fog service receives the appropriate information in the wire connection if the firewall gives access.

TABLE 3.11: TCTL properties for the functional correctness.

TCTL proprieties	**Description**
A[] sub.writing imply (sub_sec >= obj_sec) || sub_sec==Max	**Write** property management.
A[] sub.reading imply (sub_sec <= obj_sec) || sub_sec==Max	**Read** property management.
A[] sub.updating1 || sub.updating2 imply (sub_sec==Max)	**Access** property management.

TABLE 3.12: TCTL properties proper to the proposed ACM.

Chapter 4

A BIM-based framework for an Optimal WSN Deployment in Smart Building

4.1 Introduction

As we explained in the last chapter, buildings can contain devices. This deployment needs optimization from many aspects such as increasing the coverage, decreasing the cost, enhancing the protection, the low latency, etc.

Nowadays the Internet of Things (IoT) might utilize a sensor network for monitoring, preventing, and securing the building environment. The IoT network could be contained dozens, hundreds, or thousands of sensors that are connected through radio waves to share information. The role of these sensors is to sense the area and subsequently deliver the information to the base station which can relay the information into a large-scale network (eg. via the Internet). The IoT networks are densely disseminated over different geographical locations to perform their tasks such as area monitoring, processing, or data collection. However, the use of the Internet of IoT in smart buildings has great importance and promising outcomes. Researchers and industrial partners have achieved several use cases where they have leveraged various enabling technologies for service enhancement. Many application sectors as smart cities can benefit from an enhanced data collection and effective data analysis process done on data gathered from smart building devices [223]. Particularly, in the case of building monitoring and control to collect data with the aim of offering different services especially related to health, user comfort, and energy consumption.

In literature, evolutionary algorithms to solve multi-objective optimization problems attract more and more researchers in different fields of study to find the best solutions. There are various approaches to resolving this problem. One of the standard methods is the Genetic Algorithm (GA). While installing many sensor nodes takes time and costs money which includes equipment investment, installation, and maintenance. This work addresses the planning of sensor deployment by using an evolutionary multi-objective algorithm to provide optimal planning nodes positions within a building that takes the obstacle into account. The objective of this chapter is to provide the best positions to deploy sensor nodes with maximum coverage and minimum nodes deployment within the building considering the k-connectivity and impact of obstacles.

This chapter is organized as follows. We present the related work in section 4.2 and our proposed solution in section 4.3. Then, we observe the performance evaluation in section 4.4. Finally, section 4.5 concludes this work.

4.2 Related Work

In this section, we survey the literature related to WSN deployment and compare compare them with our solution. Zhang *et al.* [224] investigated how BIM could support the development of smart building environment from the architecture plan to a building management. They extended BIM for the design step to supply material profiling and the information exchange interface for different sensor objects. They also proposed a three-layer validation scheme to facilitate the BIM users determining the possible defects in the BIM plan. Chang *et al.* [225] showed how to visualize sensor data in BIM platform with multiple point of views for the purpose of supporting complex decisions requiring interdisciplinary information. The authors also discussed the design of a standard platform enabling intercommunication between sensor nodes with different protocols, and how visualization might support in energy-saving management decision-making. The approach is based on the positions of IoT nodes without optimizing the cost of BIM.

From a coverage and connectivity perspectives, the authors in [226] studied the sensor deployment strategies by considering the presence of obstacle. Moreover, in [227], the author proposed a deployment method for multiple types of requirements to address the issue of grid-based deployment and deterministic. The authors in [228] evaluated the suitable area for sensors deployment by using the signal strength in order to minimize the deployed nodes. In [229], the authors designed a model for a multi-objective optimization problems to deploy and relocate robots in indoor environments. In the work of [230], the authors proposed a multi-level strategy of genetic algorithm with the objectives of a better the coverage, a number of deployed Radio frequency identification (RFID) readers and the interference. In addition, the authors [231] proposed an evolutionary algorithm to a node deployment problem with static sensors. They consider that the relation between the genotype space and the phenotype space of the optimal sensor deployment problem can be observed in terms of quotient space.This works discusses separately the collection capacity of sensors and their communication without combining in a unified framework. Farther, they exclude the obstacles from their work. The authors in [232] proposed two metaheuristics to address WSN deployment problem in the case of smart building. They take into account the presence of obstacles like walls and doors by relying on the multi-wall model (MWM). The use of NSGA-II is recommended in their study especially when it is not a priory approach.

M Kacou *et al.* [135] presented two path loss models for a building map to the objects using the frequencies 800 MHz to 6 GHz. The first model depends on log-distance and the subsequent one is a multi-wall path loss model that integrates the log-distance with the obstacles attenuation. At this end, it is divided into: 1)a generalized multi-wall path loss model that classifies the barriers into two parts dividing walls and load-bearing walls, and the detailed multi-wall path loss model that takes the real values of the obstacles. M Kacou *et al.* [135] focus on the propagation without the sensing operation. Our work deals with the sensing by taking into consideration the distance between the sensor and the target, obstacles impact and the sensing range.

To simulate preliminary systems in a network and facilitate their management, Loizos Kanaris *et al.* [233] proposed a two steps methodology to deploy WSN and IoT networks in complex urban environments. First, it integrates the deployment in TruNET wireless then exports the obtained results from TruNET to Cooja simulator.Loizos Kanaris *et al.* [233] methodology is difficult to apply, because the Cooja simulator has a set of parameters which are difficult to configure. But in our approach, we create our simulator that is compatible with the coverage equation, the signal propagation and the chosen technique to represent the solution in a specific area of interest.

Hemant Ghayvat *et al.* [234] proposed an approach to create an adaptable sensor systems for smart building. First, it deploys the WSN nodes and IoT objects in a house to monitor the inhabitant's events by collecting the sensor's data. Then, it expands the area of interest by showing how band interference and attenuation of obstacles have a role to determine the sensors' QoS.Unfortunately, this study do not take into account the ideal positions of the sensors to increase the QoF and consequently decrease the BIM cost.

To increase the lifetime of a wireless network, Pratit Nayak *et al.* [235] developed an algorithm to evaluate the lifetime of network in the presence of obstacles. The algorithm takes into account the number of nodes, the size of the nodes, the number and positions of the obstacles and the number of rounds. Pratit Nayak *et al.* [235] do not consider the communication part to augment the lifetime of a network.

In our case, we focus on both the communication and the connectivity of the WSNs that is based on the signal propagation on obstacles. With respect to the surveyed literature, this work exploits BIM to improve sensors deployment inside smart buildings. The developed framework is implemented to be a plugin with any BIM supported tool. Further, the framework develops a multi-objective evolutionary algorithm in order to improve the indoor coverage while taking into account several types of obstacles. The framework produces automatically the optimal deployment as well as it is extensible to cover more parameters as well as takes the online modification on BIM data base.

4.3 Indoor Sensor Optimal Deployment Framework (ISOD)

The main goal of integrating data management and control in smart buildings is to combine multiple technologies, automated controls, and decision-supporting techniques to provide a rapid and responsive environment. The achievement of this goal is closely related to the use of the Internet of Things (IoT) [146]. In fact, IoT mobilizes advanced technologies to monitor various environmental measures such as temperature, humidity, light and motion, to analyze the operational efficiency of building systems, and to optimize facility operations using data intelligence gathered in real-time. Among these technologies, there are sensors combined to cloud software platforms allowing managing, automating, and controlling the systems remotely.

Nevertheless, before the data collection phase, it is necessary to optimize the deployment of sensors inside the building to ensure better coverage. However, the deployment issue becomes more complex when dealing with a larger building containing several types of obstacles. For a good monitoring system, sensors should be placed in an optimal position within the building to regulate the coverage and connectivity issues. Therefore, it is important to find an adapted solution that automatically provides an optimal nodes deployment by maximizing the coverage and connectivity while minimizing the number of deployed nodes. With accurate data, we could enhance the energy efficiency of building systems like HVAC [236]. It is a well-known fact that buildings consume about 40% of the energy consumption in the world.

Building Information Model (BIM) is a process of developing a digital equivalent of an actual building in terms of its physical and functional characteristics that supports data exchange, management and communication during the whole building's life cycle. Resource allocation and reduction are major drivers toward BIM implementation, whether it be using renewable or recycled materials or reducing energy consumption [237], [225]. Not only the BIM afford manufacturers, designers, and integrator advantages in design efficiency and quality control, but also, it improves communication within the design and construction teams as well as the parametric elements of the model by creating a robust database. The latter contains mainly physical information (such as material, size, and living space) about the building. Leveraging this data means that optimal sensors deployment can be created from the parametric model elements.

Despite the potential amount of data, the deployment of sensors in an indoor context supporting heterogeneous obstacles is a difficult problem [238].

Figure 4.1 illustrates the steps needed to deploy an optimal configuration in a smart building with maximum signal coverage and a minimum cost. In ISOD, the system's architecture is composed of a set of smart objects, physical properties and plans, and connectivity including the used communication protocols. The nodes are active/passive objects to collect the needed environmental measurements. The communication protocols ensure how well the connection between nodes is established where the measured data are packed and encrypted. The physical architecture separates the locations with different types of separators that can absorb signals with multi-scale values depending the used material in separators. The analysis step looks for the best nodes distribution that satisfy the defined objectives which is a trade-off between coverage, connectivity and cost. Finally, the results show and simulate the deployment of the optimal configuration.

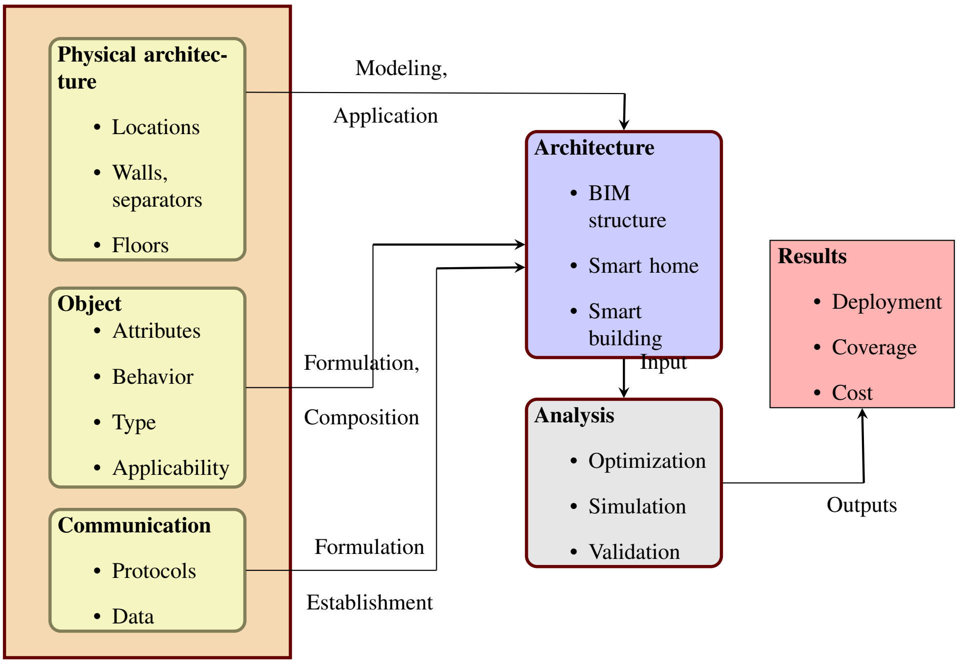


FIGURE 4.1: Indoor Sensor Optimal Deployment Framework.

4.3.1 Smart building architecture

We define a smart building `sEnv` as a structured physical infrastructure (building or home) that carries smart nodes. `sEnv` is composed of at least two smart rooms/locations disjointed by separators *like* walls, doors, and windows of different form, size, and materials. To collect information and sensitive data, smart nodes are connected with a network based architecture that helps them to communicate easily through a dedicated protocols. Definition 4.3.1 illustrates formally a general smart environment.

[Smart Environment] A smart environment `sEnv` is a tuple of $\langle E, L, \mathbf{SoT}, \mathtt{PL}, \mathtt{DL} \rangle$, where:

1. E is the environment's label,
2. $L = \{l_i : i > 0, i \in \mathbb{N}\}$ is the set of locations/rooms (l_i) composing E,
3. $\mathbf{SoT} = \{\mathtt{SoT_i} : \mathtt{i} > 0, \mathtt{i} \in \mathtt{N}\}$ is the set of smart nodes in E,
4. `PL` is a graph structure that defines the physical structure of E,
5. `DL` is the logical architecture that connects **SoT** in `PL`.

As example, Figure 4.2 shows the physical structure of a smart building consisting of least smart rooms (l_i and l_j). <PL> defines the physical characteristics of the separator between l_i and l_j such us: type, quality, and position. Further, Figure< 4.3 shows the logical structure connecting smart objects (SoT_i) that uses a range of communication technologies (DL).

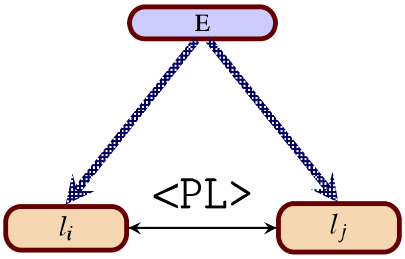


FIGURE 4.2: The physical structure of a smart home.

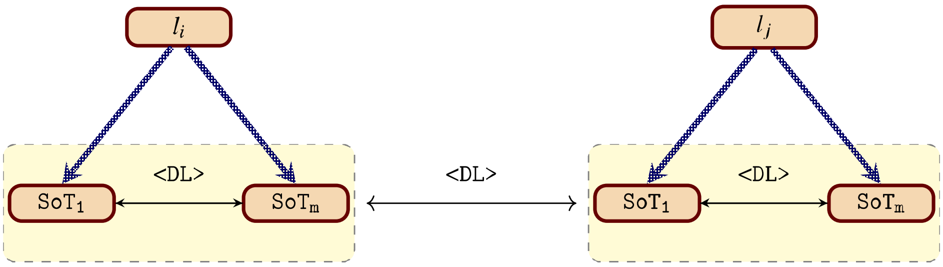


FIGURE 4.3: The logical structure of a smart home.

Both structures are merged in one environment and formatted as XMI files in BIM database. The visualization of a BIM file is showed in Figure 4.4.

4.3.2 Problem Formulation

ISOD assumes that the building plan is depicted as a Virtual Grid Architecture (VGA) composed of cells of $1m^2$. An abstract sensing model is considered stating that if the cell lies in the sensing region it will be covered with a probability between 0 and 1, unlike the existing initiatives that use only a binary sensing model to compute the sensing coverage. ISOD also considers that sensors are represented by a disc graph model where the radius is equal to the sensing range Rs. Each sensor node is located at the center of gravity of the cell and collects information inside this circle particularly if there is not obstacles. In the case of obstacle, a deformation of the circle is considered.

To achieve more coverage precision, we take into account the presence of obstacles while differentiating between materials that compose them. As stated before, these information are exported from the BIM database that defines the building plan, the used materials, and how they are composed. The Composition contains information about the structure of a building element (walls), by defining composition layers. Each composition layer refers to a building material characterized by an energy performance with a certain thickness.

In the present solution, ISOD focuses on static and homogeneous temperature sensors. The aim is to maximize the covered area of the sensor field with the minimum number of nodes. To solve this multi-objective optimization problem taking into account the presence of walls, we propose a new implementation of NSGA-II algorithm that requires to design the objective functions in order to evaluate the quality of solutions with respect to the connectivity and cost constraints. Our coverage objective function is based on two criteria: the distance between the sensor with the target cell and the R-value. The R-value measures the heat flow resistance of a given material and it means how much the heat can be transferred regarding its thickness and physical properties. The higher the R-value of a material is, the more effective it is as an insulator. The R-value is measured in meters squared Kelvin per Watt (m^2K/W) calculated by using the formula 4.1 Where l is the thickness of the wall (obstacle) in metres and λ is the thermal conductivity in W/mK.

$$R = \frac{l}{\lambda} \tag{4.1}$$

For example, the thermal resistance of some types of materials are presented in Table 4.1 according to their thickness.

To ensure the connectivity robustness, reliability and load balancing level, the WSN of each deployment is k-connected, where k is defined according to the needs and the areas of application. The proposed mechanism is based on a multi-wall propagation model, which will be described in Section 4.3.4. We consider in this model that a radio signal is attenuated when it crosses obstacles.

4.3.3 Deployment sensing coverage and cost

Let $\mathbb{B} = \{0,1\}$ a set of values, active (1) or not (0), for the sensor nodes in a grid $\mathscr{G} \in \mathbb{B}^{m\times n}$ of $m \times n$ cells where g refers to the deployed node in its position $(i,\ j)$ such that:

$$g_{ij} = \begin{cases} 1, & \text{if node } g_{ij} \text{ is active} \\ 0, & \text{otherwise} \end{cases} \tag{4.2}$$

Coverage is an important factor related to WSN quality of service. Our solution attributes a cost of value between 0 and 1 to each cell in order to estimate precisely the deployment coverage ratio. The cost of a given cell is calculated by relying on the distance separating the cell of interest and the one where the sensor is located as well as the impact of any existing obstacles between them. A cell c_{ij} is covered by a sensor g_{kl} situated in the cell c_{kl} only if the distance between the centroid of both cells c_{ij} and c_{kl} is less or equal to the sensing range R_s of g_{kl} while respecting the thermal conductivity constraint of the separators between c_{ij} and c_{kl}. ISOD initiates the cost of all cells to be null with a random deployment of sensors.

Based on this random distribution, the cost of cells is calculated using Equation 4.3 and the information retrieved from the BIM database.

$$s_{kl} = \begin{cases} max(\frac{R_s}{(\|\hat{c}_{ij}-\hat{c}_{kl}\|*exp^{\sum_{d=0}^{w} R_d})+R_S}, s_{kl}), & \\ & if \|\hat{c}_{ij} - \hat{c}_{kl}\| \leq R_s \\ s_{kl}, & \text{otherwise} \end{cases} \tag{4.3}$$

$\forall i \in [1,m]$, $\forall j \in [1,n]$, $\forall k \in [max(1,i-R), min(m,i+R)]$, $\forall l \in [max(1, j-\sqrt{R^2-k^2}), min(n, j+\sqrt{R^2-k^2})]$, we have: $\hat{c}_{ij} = \begin{pmatrix} (i-1)*\hat{c} \\ (j-1)*\hat{c} \end{pmatrix} + \begin{pmatrix} \frac{\hat{c}}{2} \\ \frac{\hat{c}}{2} \end{pmatrix}$.

Here,$\|\hat{c}_{ij} - \hat{c}_{kl}\|$ is the Euclidean distance between the centroid of the cell g_{ij} (c) where the sensor is placed and the target cell g_{kl} $(\hat{c})$ where the cost should be computed. Farther, R_d is the thermal resistance of a separator and w is the number of obstacles existing between both cells c_{ij} and c_{kl}. Thus, each cell c_{kl} in the target area is associated with a maximum value, denoted g_{kl} and $0 \leq g_{kl} \leq 1$. The final cost value of a cell c_{ij} takes the maximum cost values of all neighbour sensors by considering their distances from the centroid of c_{ij} as well as the existing obstacles impacting the sensing. The case where a cell has a sensor, the cost has a maximum value of 1.

As stated above, ISOD is based on NSGA-II algorithm to find the best sensors deployment where all the objective functions and the constraints should be satisfied. Hence, Equation 4.4 describes the objective functions used by our algorithm to solve the coverage and the cost problems.

$$\begin{cases} F_{cov}\text{: maximizes the deployment coverage.} \\ F_{cos}\text{: minimizes the cost of the solution.} \end{cases} \tag{4.4}$$

where:

$$\mathscr{F}_{cov} = \max \sum_{k=1}^{m} \sum_{l=1}^{n} s_{kl} \tag{4.5}$$

and

$$\mathscr{F}_{cos} = \min \sum_{i=1}^{m} \sum_{j=1}^{n} g_{ij} \tag{4.6}$$

The function $\mathscr{F}_{cov}$ (eq. 4.5) measures the sum of costs evaluated for each cells to select the maximum coverage that represents the best deployment solution. Whereas, the function $\mathscr{F}_{cos}$ (eq. 4.6) minimizes the number of active sensor nodes g_{ij} in the deployment plan. Consequently, the cost of the deployment is reduced as well. In a such given solution, all nodes should be well connected (see Section 4.3.4).

4.3.4 Connectivity

To store and analyze the collected data, nodes should be well connected to communicate by forming a connected graph. ISOD verifies if a node has at least a path to reach the sink node and ensures that all nodes are structured as a connected graph $G(V,E)$ where V is a set of nodes and E is a set of connections that determines the k-connectivity graph G for each deployment denoted by $Conn(G)$ s.t.: $Conn(G) = min(degree(V))$. We say k-connectivity in a graph G where $k \geq Conn(G)$.

To achieve a k-connectivity, we calculate RSS (the received signal strength) by relying on Multi-Wall Model (MWM) [135] that considers the degradation of the transmitted signal through obstacles between a transmitter and a receiver sensor. One of the impact on the signal quality during its propagation in a floor environment is the path loss that measured in dB by Equation 4.7, where k_w is the number of the wall types, k_{wi} and L_{wi} denote the number and the loss of the i^{th} wall type, respectively.

$$L_{dB} = L_{0,dB} + 20log_{10}d + \sum_{i=1}^{K_w} K_{wi}L_{wi} \tag{4.7}$$

The free-space path loss (FPL) in linear scale is given by:

$$L_0 = (\frac{4\pi d_0}{\lambda})^2 \tag{4.8}$$

ISOD adopts this model to take into account the characteristics of obstacles extracted from BIM database (Brick, Wood, Glass) that have a direct impact on the signal shadowing.

4.3.5 Evolutionary Genetic Algorithm

In the genetic algorithm, a binary encoding scheme is used to represent the chromosomes [239]. A chromosome, attributed as a component of an *individual* in a *population*, is formed by a developing set of genes. A population is constructed by a determined number of chromosomes.

The evolutionary genetic algorithm follows mainly three steps:

1. Define an adequate deployment, *chromosome*.
2. Create randomly a set of chromosomes, *population* .
3. Apply the reproduction operators (*selection, crossover, mutation*) to simulate the natural evolution.

ISOD-NSGA populations are the deployed sensors in an area of interest. Algorithm 3 initiates a deployment (line 1) as shown in Figure 4.5 where the area of interest is a rectangle of length (L) and width (W) divided into cells of surfaces 1 square meter. Each cell can has a sensor in its centeroid ($g_{ij} = 1$) or not ($g_{ij} = 0$). A chromosome representation transforms the matrix into an array of length Lchrom, where: L_{chrom} = W*L.

After the population initialization, Algorithm 3 evaluates the quality of each configuration by applying both objective functions $\mathscr{F}_{cov}$ and $\mathscr{F}_{cos}$ in order to rank each chromosome (line 2). To achieve an optimal deployment, we select the two best chromosomes according to their ranks satisfying the connectivity constraints (line 4). Then, Algorithm 3 generates a new chromosome through crossing and the mutation procedures.

To improve the quality of the resulted deployment by Algorithm 3, ISOD built a second algorithm called "Optimize Positions Sensors" (OPS) (Algorithm 4) that runs in two steps: 1) eliminate the sensors having no impact to avoid the over covering case, and 2) search a new position for each sensor in the square area (of dimension $2R_s$*$2R_s$) in order to enhance the obtained deployment.

Algorithm 3: ISOD-NSGA

```
initialize population                                          // Random deployments
Evaluate Individual fitness                 // calculate the rank for all chromosomes
for $i \leftarrow 1$ to $MaxGener$ do
                                              // $MaxGener$ is the number of generation
    Select Ranked Individuals
    for $j \leftarrow 1$ to $Offspring\_Pop$ do
        Select Parents
        Crossover Or Mutation
        Offspring Evaluation  // Satisfy MWPLM and K-connectivity constraints
          & calculate the rank
    end
    Rank(parents + Offsprings)
end
Call OPS
```

4.4 The experimental results

Our experiments run on different indoor environments by taking into consideration: sensors positions and their types, and more importantly the connectivity. Table 4.2 illustrates the initial values of parameters used in Equation 4.7. Also, it gives the impact of three type of obstacles on a signal attenuation in dB.

4.4.1 The first scenario

The first experiment looks for a solution on an empty space of dimension L=12m, W=10m, and Rs=3m. Figure 4.6 shows the generated solutions where $\mathscr{F}_{cos}$= 6 sensors and $\mathscr{F}_{cov}$= 100% which is the best configuration (green plot) in terms of the coverage compared to the other ones presented in Diagram 4.7 that describes all possible solutions (blue plots) in terms of coverage ratio and the number of sensors.

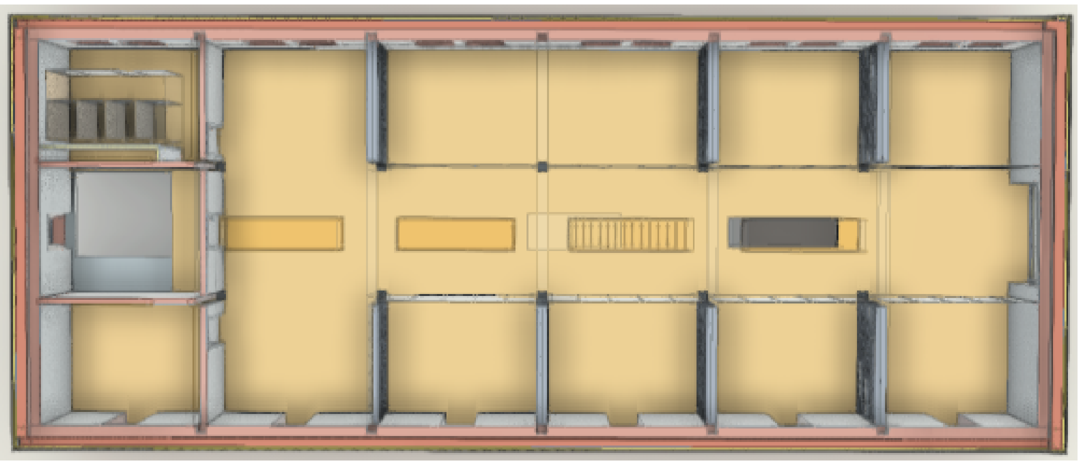


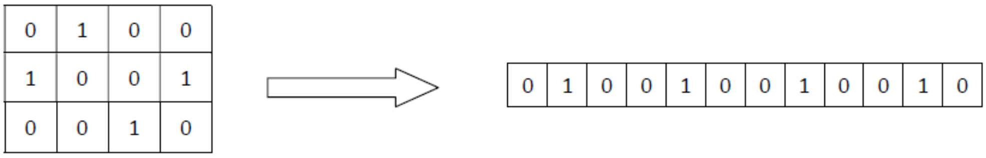
FIGURE 4.4: A BIM Floor Visualisation.

TABLE 4.1: Thermal resistance of various obstacle materials.

Obstacle	e (meter)	λ	R	Colors
Brick	0.2	0.156	1.28	black
Wood	0.04	0.14	0.46	yellow
Glass	0.01	0.038	0.43	blue

Algorithm 4: OPS

```
for $i \leftarrow 1$ to $L * W$ do
                                            // Delete additional Sensors
    delete(Sensor(i))
    if $New\_cov < Old\_cov$ then
        recovery(Sensor(i))
    end
end
for $i \leftarrow 1$ to $L * W$ do
                      // Search new position in area $2R_s * 2R_s$ of each sensor
    Take New Sensor
    for $k \leftarrow 1$ to $2R_s$ do
        for $l \leftarrow 1$ to $2R_s$ do
            Max(Sensor(i), Coverage(position(k,l)))
        end
    end
end
```



0	1	0	0
1	0	0	1
0	0	1	0

0	1	0	0	1	0	0	1	0	0	1	0

FIGURE 4.5: Representation of a chromosome.

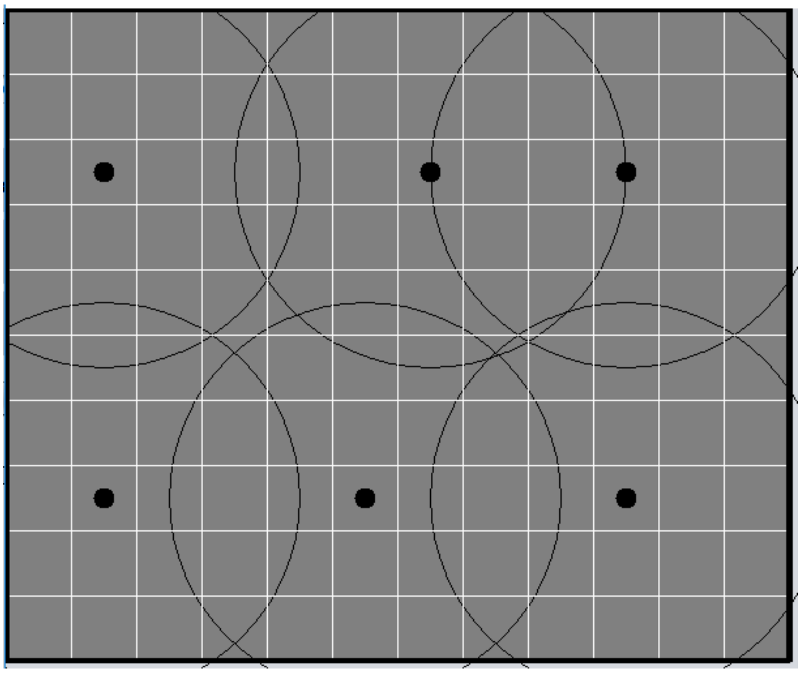


FIGURE 4.6: The best deployment in scenario 1 (free space).

4.4.2 The second scenario

This experiment shows how our ISOD automatically handles the obstacles and the connectivity constraint with respect to the thermal resistance and the attenuation communication signal of the chosen obstacles represented in 4.1 and Table 4.2, respectively.

While fixing the connectivity constraint to 1, we develop two other environments rather than

TABLE 4.2: Signal Strength Parameters.

Symbol	Value
Tx	-11 dB
Rx	-70 dB
L_0	40.2 dB
Brick	4 dB
Wood	3 dB
Glass	2 dB

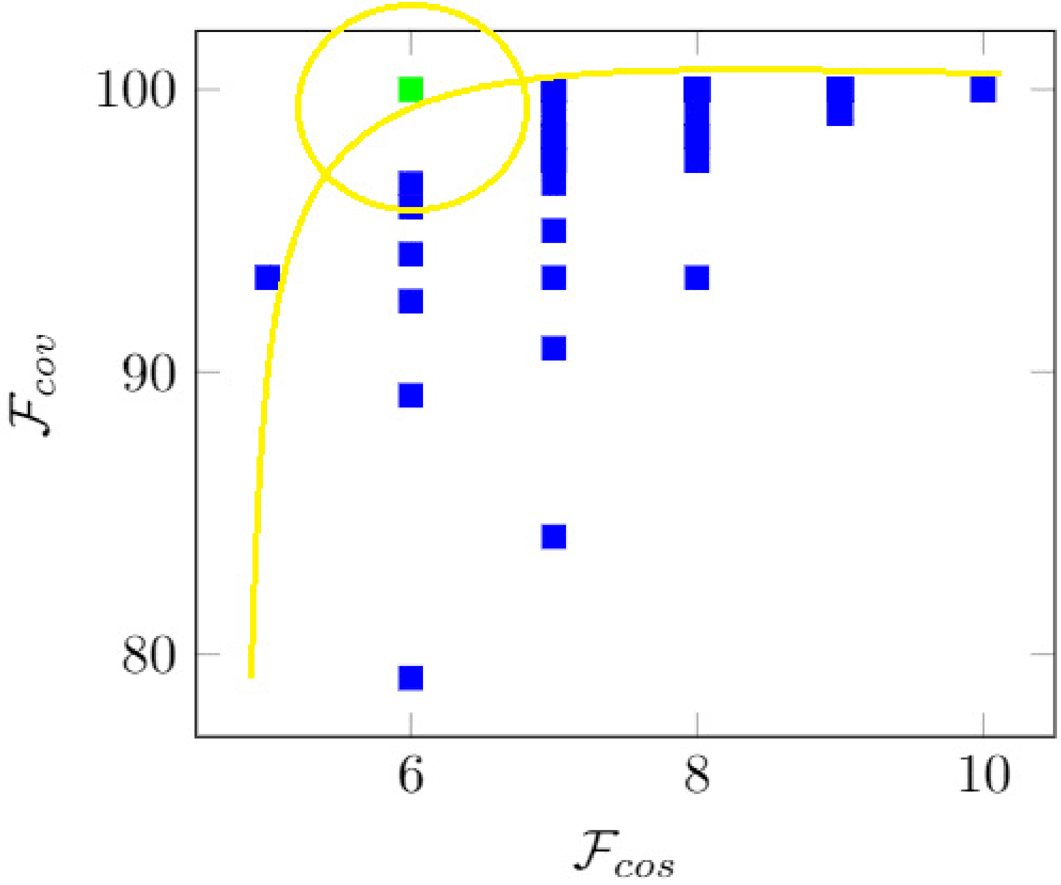
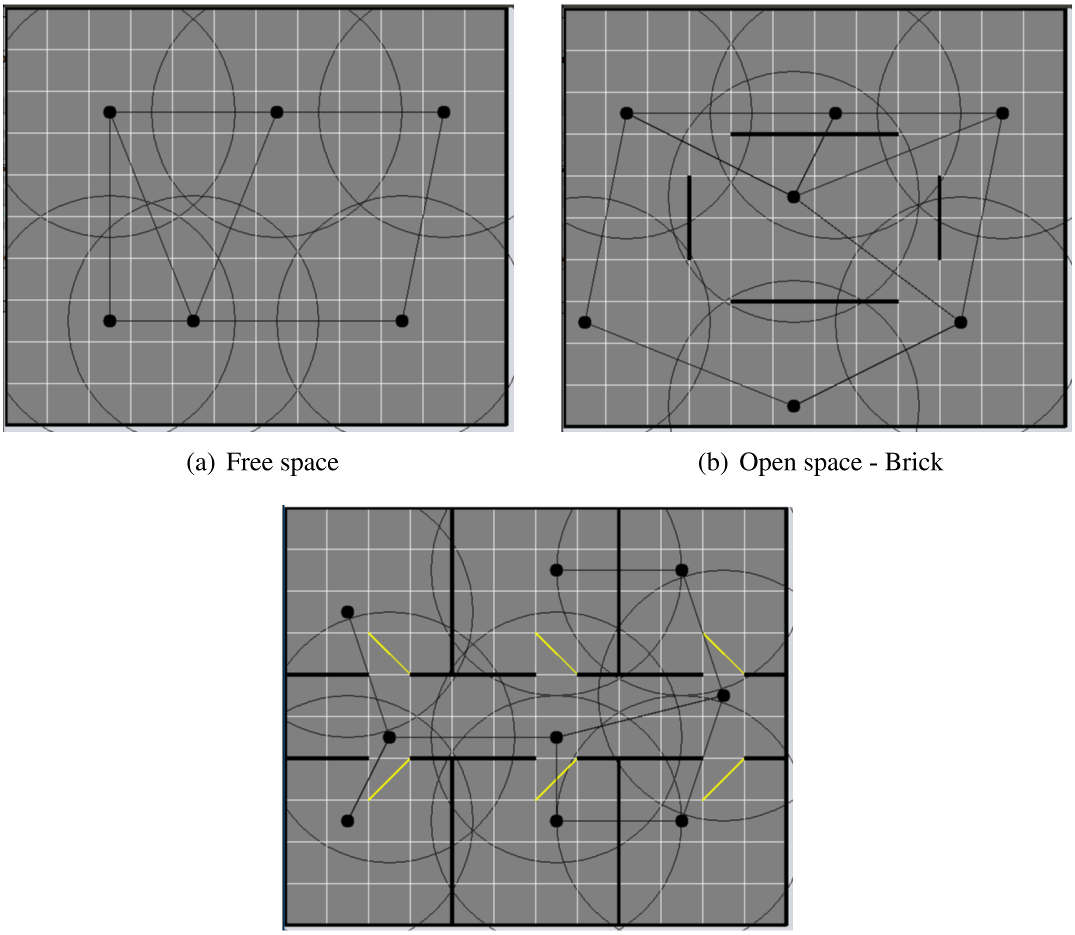


FIGURE 4.7: The generated solutions for scenario 1 (free space).

the free space one depicted in Fig.4.8(a) . The new environments presented in Fig.4.8(b) (open space) and Fig.4.8(c) (closed space) have different position and number of obstacles. The obtained deployment for the free space has $\mathscr{F}_{cos}$ = 6 and $\mathscr{F}_{cov}$ = 100%), and for the open space has $\mathscr{F}_{cos}$ = 7 and $\mathscr{F}_{cov}$ = 100%, whereas the one for the closed space has $\mathscr{F}_{cos}$ = 9 and $\mathscr{F}_{cov}$ = 100%. . It is clear that ISOD adapt dynamically the sensors deployment for different positions and number of obstacles while respecting the connectivity condition and assuring a maximum coverage (100%).

When the connectivity is 2 for the same environment, we obtain $\mathscr{F}_{cos}$=6 and $\mathscr{F}_{cov}$=100% for the free space (Fig. 4.9(a)), $\mathscr{F}_{cos}$=7 and $\mathscr{F}_{cov}$=100% for the open space (Fig. 4.9(b)), and $\mathscr{F}_{cos}$=11 and $\mathscr{F}_{cov}$=99.17% for the closed space (Fig. 4.9(c)).

By comparing the results obtained by the experiments wherek_{conn}=1 and k_{conn}=2, we found that there the positions of sensors have been changed for the three environments. ISOD results show a maximum coverage ratio with a minimum number of nodes except the case shown in Fig.4.9(c) due to the important number of obstacles.



(a) Free space

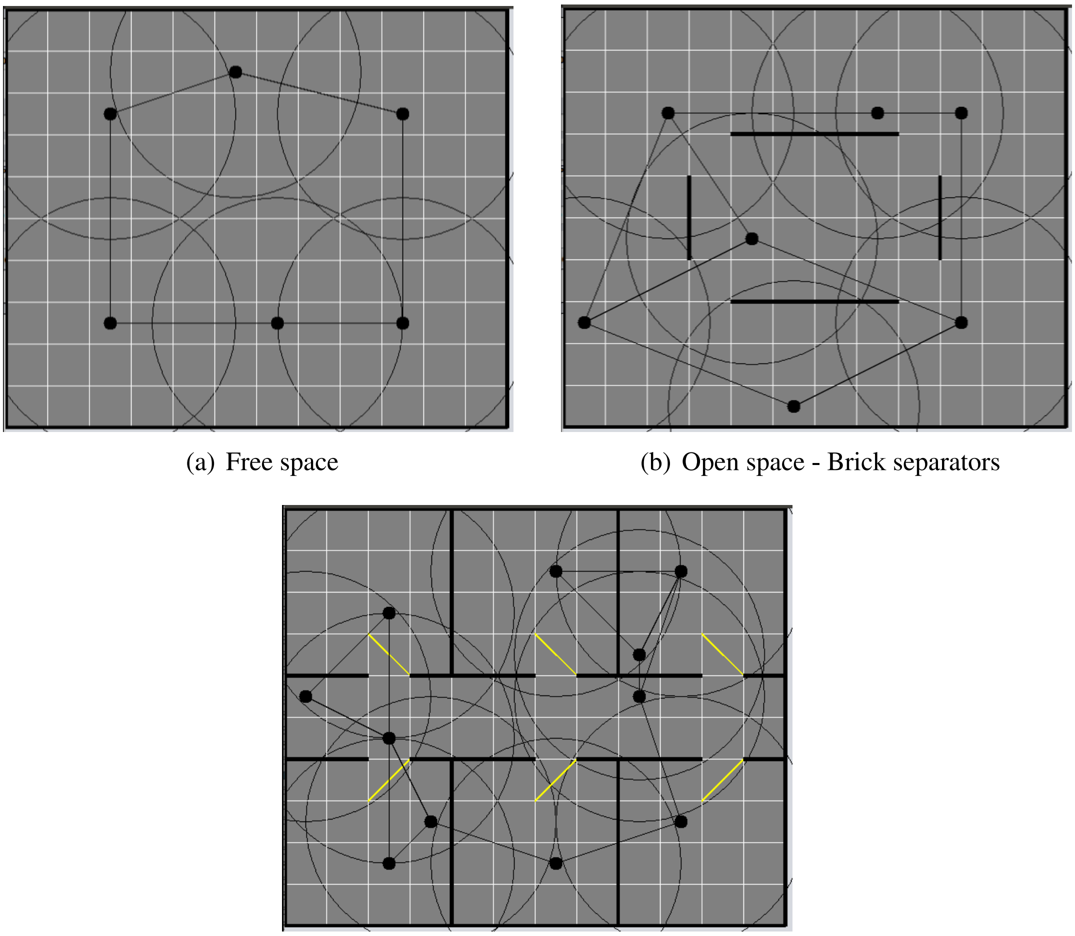
(b) Open space - Brick

(c) Closed space - Brick and wood

FIGURE 4.8: The best deployment in scenario 2 (10m *12 m) with k_{conn}=1.

We conclude that our scheme increases the number of sensors only if needed to respect $k-$connectivity constraint and achieve the target coverage.

After running the same experiments with k_{conn}=3, we obtained results $\mathscr{F}_{cos}$=7 and $\mathscr{F}_{cov}$=100% for the first environment (Fig.4.10(a)), $\mathscr{F}_{cos}$=9 and $\mathscr{F}_{cov}$=100%) for the open space (Fig. 4.10(b)), and $\mathscr{F}_{cos}$ = 14 and $\mathscr{F}_{cov}$ = 98.33% for the closed space (Fig. 4.10(c)). From this experiment, we observe that the number of sensors has been increased when k_{conn} became 3 for the different cases (free, open, and closed space). We found that even the strong constraint of the connectivity, ISOD find the best deployment solutions in terms of the number of nodes and the coverage ratio.



(a) Free space

(b) Open space - Brick separators

(c) Closed space - Brick and wood

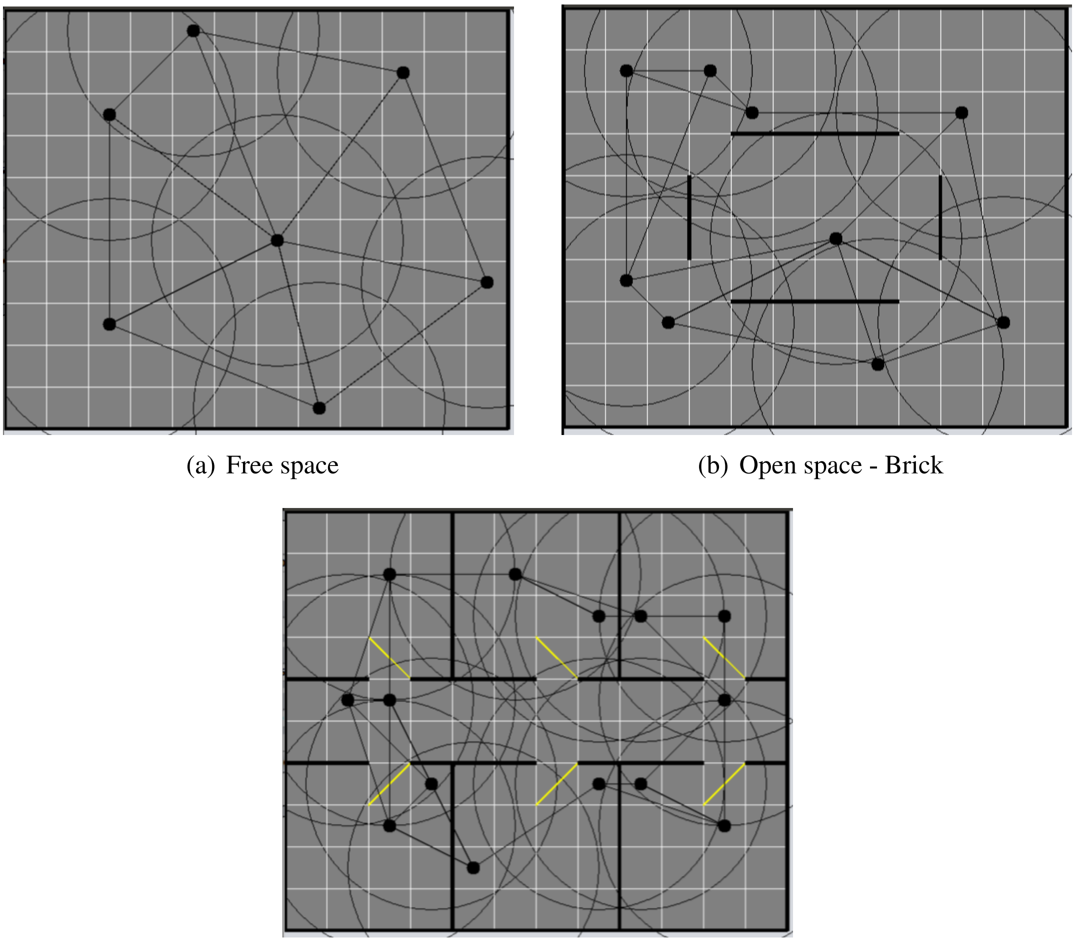
FIGURE 4.9: The best deployment in scenario 2 (10m *12 m) with k_{conn}=2.

4.4.3 The third scenario

In this scenario, we increase the environment surface to 15 * 20 m^2 for free and closed spaces. For the closed space, we keep the same positions of obstacles but we change their type from glass (4.11(b)) to brick (4.11(c)).

For a range sensing of Rs=3m and k_{conn}=1, the obtained results are $\mathscr{F}_{cos}$=15 and $\mathscr{F}_{cov}$=98.67%) for the free space (Fig. 4.11(a)), $\mathscr{F}_{cos}$=16 and $\mathscr{F}_{cov}$=98.33% for the closed space with glass separators (Fig.4.11(b)), and $\mathscr{F}_{cos}$=19 and $\mathscr{F}_{cov}$=98.00% for the closed space with the brick separators (Fig.4.11(c)).

From the obtained results, we found that only one more sensor has been added to the case of closed spaces but the locations of sensors have been changed to keep the same coverage ratio.



(a) Free space

(b) Open space - Brick

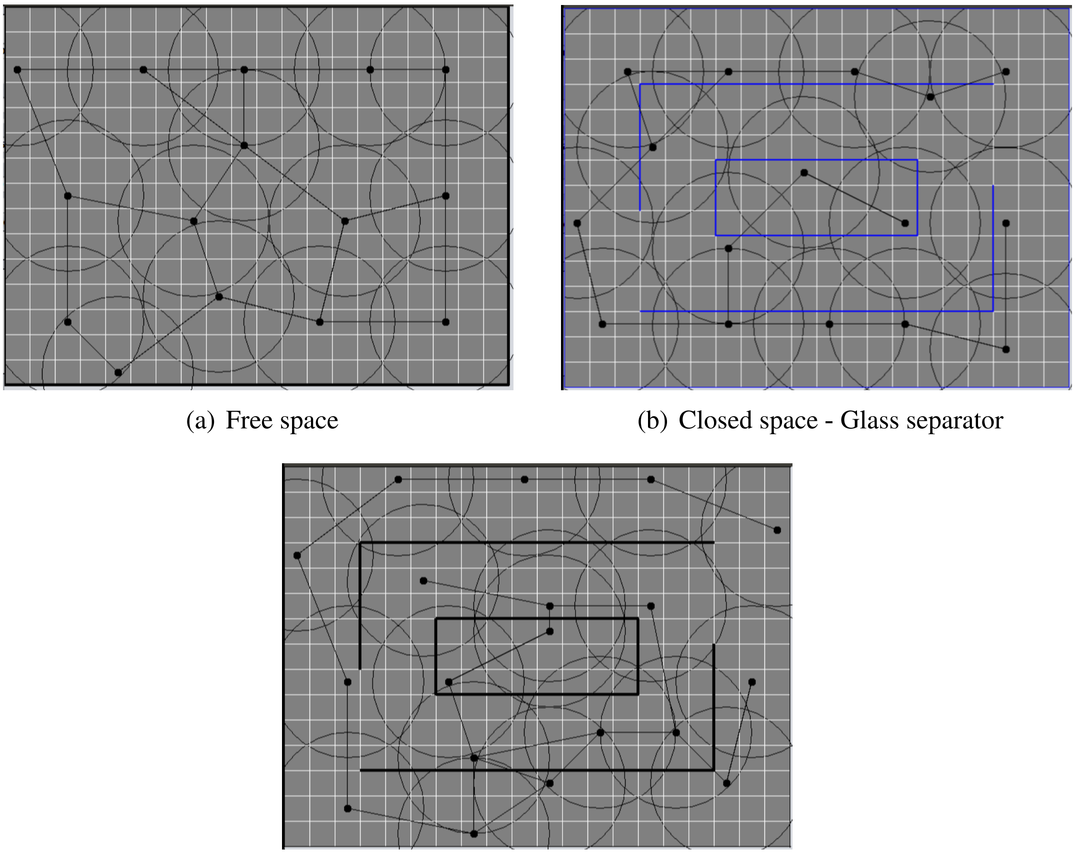
(c) Closed space - Brick and wood

FIGURE 4.10: The best deployment in scenario 2 (10m *12 m) with k_{conn}=3.

Further, the obtained deployments show that our solution take into account the thermal resistance and thickness of the different type of separators.

We notice that the number of sensors increases with respect to the obstacles impacts. Thus, the results are more satisfactory since there is no grouping of sensors except beside the obstacles. Farther, the level of the coverage is large in the three zones and the constraint k_{conn} is respected. Then, we conclude that the algorithm is scalable.

We notice that the number of sensors increases with respect to the obstacles impacts. Thus, the results are more satisfactory since there is no grouping of sensors except beside the obstacles. Farther, the level of the coverage is large in the three zones and the constraint k_{conn} is respected. Then, we conclude that the algorithm is scalable.



(a) Free space

(b) Closed space - Glass separator

(c) Closed space - Brick separator

FIGURE 4.11: The best deployment in scenario 3 (15m *20 m) with k_{conn}=1

4.4.4 The fourth scenario

In this scenario, we compare the obtained deployment from the third scenario and represented in Fig. 4.11(c) (where $\mathscr{F}_{cos}$=19 sensor and $\mathscr{F}_{cov}$=98.00%) with another 15 random deployments. First, we fix $\mathscr{F}_{cos}$ to 19 sensors and generate random solutions with the same number of nodes. Then, we compare the coverage ratio for the generated deployment of each solution with the one produced by ISOD. Fig. 4.12 represents the coverage ratio of our solution (solution n=1) compared to the other 15 random ones. We found that our solution has the better coverage with the same number of nodes.

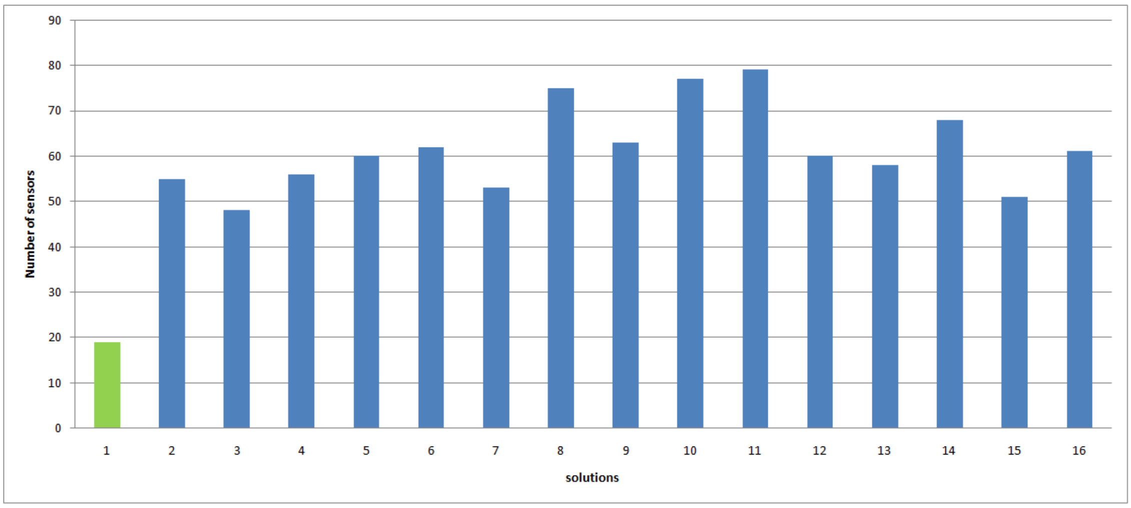


FIGURE 4.12: The number of the sensors where $\mathscr{F}_{cov}$=98.00%.

In the second test, we fixe $\mathscr{F}_{cov}$ to 98.00% then we generate random solutions in order to reach a fixed coverage ratio. Fig. 4.13 represents the minimum number of sensors used by our deployment as well as the other random solutions. ISOD deploys only the necessary number of nodes to cover a 98% of the target area. In contrary, the other solutions use a considerable number of sensors to achieve the same coverage ratio. Consequently, ISOD reduces the deployment cost.

4.5 Conclusion

In this chapter, we have developed a framework called ISOD to automatically deploy WSNs in smart buildings by exploiting BIM database. The framework built an evolutionary algorithm

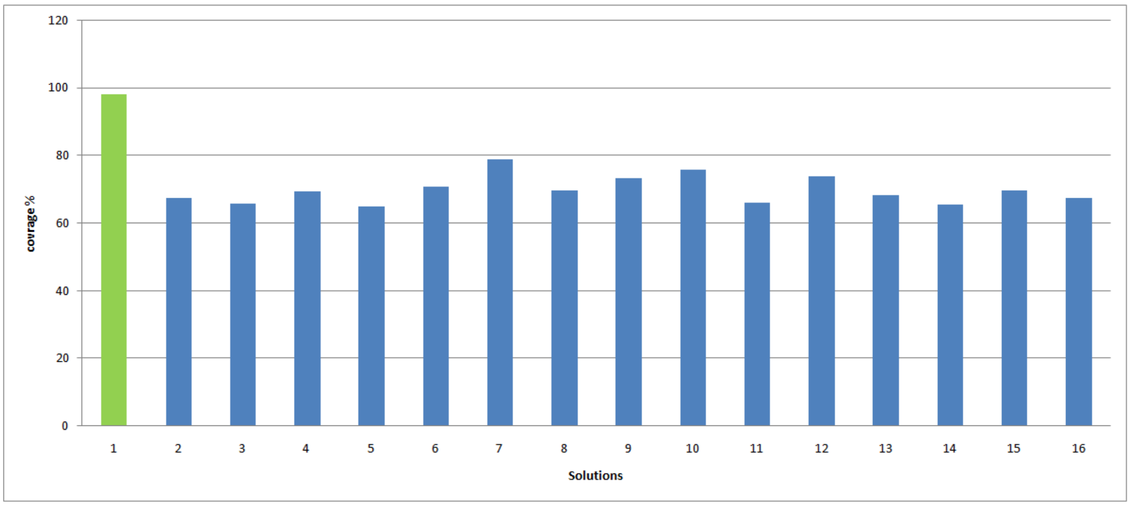


FIGURE 4.13: The coverage ratio comparison for $\mathscr{F}_{cos}$=19.

(NSGA-II) to produce an optimal deployment by solving a multi-objective function that minimizes the number of sensors and maximizes their covered areas. To assure a *k*connectivity, ISOD adopts the multi-wall model (MWM) to measure the signal strength on different types of obstacles. Moreover, to improve the quality of solutions, we proposed a second algorithm (OPS) that optimizes the obtained results. In the next chapter, we will increase the protection level of the smart city, it addresses two issues the integrity of data and the access control through the blockchain.

Chapter 5

Protection the Smart City System

5.1 Introduction

As we explained earlier, the city is witnessing a continuous flow of data, so, the sustainability of the digital system in the smart city is very important. Many cyber threats may paralyze the proper functioning of the whole system, causing a loss of service for users. The goals of hackers differ, but the result is the same, which is corrupted information, unauthorized access to devices, DDoS attacks, spoofing attacks, sniffing attacks, etc. That is why researchers had to devise high-performance defense mechanisms to prevent or reduce these risks. The structure of the blockchain and its framework depends on the purpose of the application's domain. Many questions are about the possibility of adopting this successful technology in the smart city, in order to mitigate the cyber attacks which threat the integrity of information, especially after the terrible number of the cyber criminals.

The proposed framework should be without or with few weaknesses, scalable and compatible with the characteristics of IoT devices such as the limitation of the capacities, latency, IoT protocols, WSNs, etc. With the $IntegrityofInformation$ issue, our framework develops two concepts, the *independence* of the users and their lack of an intermediary party, also the possibility to *detect* the criminals and prevent their goals, because the dominance of the attackers in the network (more than 50% attackers) makes the network loss its reliability. So the technology is double-edged, despite the great protection it grants, it is difficult to recover it in case of damage. Hence, our proposed solution includes the advantages of the blockchain and provides mechanisms to increase its robustness. Also, with the $AccessControl$ issue, its proposed framework should touch two steps, firstly the user must determine the effective parameters in the system, such as subjects (users), object and tasks. Secondly, it must enact access policies, stipulating that they be logical and not contradictory to reality. Finally, it has to introduce the system sensitive values into the blockchain and include the access policies inside the smart contracts.

This contribution is organized as follows. section 5.2 presents a group of contributions related to our field of work. Then, section 5.3 provides the basic concepts about the blockchain technology, and section 5.4 explains our proposed methodology. Performance evaluation was shown in section 5.5. Finally, our contribution and the obtained results are summarized in section 5.6.

5.2 Related Work

In this section, we review the literature related to the blockchain technology in the various fields by identifying their weakness and strengths.

For example, in the education field, Lizcano *et al.* [240] proposed a model that was suggested for higher education students, the test was evaluated in a real environment and its results were acceptable. Tanweer *et al.* [241] proposed an educational system based on the internet of things supported by blockchain technology, the framework brings together all of the actors, students, teachers, employers, developers, facilitators and accreditors on the Internet. In addition, online education faces obstacles such as the absence of the privacy, lack of certified results certificate, and robot's participation. Thus, blockchain technology can be combined to solve these problems [242].

In the healthcare field, Celesti *et al.* [243] proposed a methodology for nursing the patient from the technicians and sending the data to a unified cloud where doctors diagnose the patient and suggest medical solutions, this system was protected by blockchain technology and was implemented on the Etheriem platform. Rathee *et al.* [244] protected health sector information with this technology, as their hypothesis was validated by simulating a group of attacks, with a success rate of 86%. As for the financial sector, Marijn *et al.* [245] have incorporated the same technology that captures the complex relationship among institutional, market and technical factors, which were interacting with each other. It was not limited to these fields only, but also included other domains such as transportation [246], the government [247] and others.

In addition, the blockchain technology is used in many domains, for example Raikwar *et al.* [136] adopted it to achieve the security of the insurance platform, where the transactions process as a smart contract. They implemented the framework on Hyperledger fabric, the results obtained showed that, it is necessary to chose the parameters which constructed the blockchain in order to optimize the network latency. On other hand, the database does not respect the privacy because the data recorded are without encryption. While, Liu *et al.* [137] proposed a framework of data integrity service, their goal is to create a reliable system that checks the data integrity without third party. Also, Li *et al.* [138] gave a crowdsourcing system, which receives the tasks from the requester and share them between the workers to solve them, the framework does not consist on third part. The tests show that the system is scalable and applicable.

Nagothu *et al.* [139] suggested a secure smart service consists on the microservices model and blockchain mechanism, their goal is to make a reliable decentralized system and give a tamper proof of data in the insecure system. The idea is as follows, each microservice records its collected information in its dedicated database. Then, the master database combines these memorizations, after that the miner node extracts its hash which will be added in the new block of the blockchain. They used the smart contract to give the authorized access to the videos captured by the surveillance cameras, the fogs that are near to the edge process in the real time the videos of the cameras, while the cloud computing performs high protection tasks as the reorganization and discovering the malicious intents. The contribution lacks the application and analysis of the obtained results to confirm the effectiveness of the proposed hypothesis. They did not give examples to support the hypothesis, such as object-recognition algorithms, security protocols and hashing mechanisms.

Sergii *et al.* [140] applied the Rolling Blockchain concept to the WSNs deployed in the smart city. The proposed network is considered as distributed servers, where, they contain the blockchain of their sub-clusters and the total blockchain. Since, the WSNs have a low capacity memory, the size of the blockchain depends on the parameters of the "worst" memory node. They gave the mathematical model for the complete chain and the segment of the chain that is removed from the original chain. They constructed a linear distribution of sensors in order to conclude if the network find a new path between two WSNs after the randomly removing of the links. Thus, when they increased the level of attacks (proportion of edges removed), the network always creates an alternative paths until its break down, so the WSN network is scalable. The experiment part did not test the integrity of the data recorded in their proposed blockchain structure. The recording of the blockchain in the WSN makes the network constrained by the worst sensor. The proposed network structure imposes the sensors to apply the blockchain operations (verification, confirmation and storing) that affect the energy storing, the processing and the memorizing capacities which are limited in the sensors.

Jia *et al.* [141] concerned with increasing the level of protection on the crowd sensing network by the blockchain technique. The network consists of three parts, intelligence crowd sensing networks, confusion mechanisms, and blockchain. The crowd sensing network contains sensors to collect the information users that will be sent to the confusion mechanism. This latter regroups the sensors into 10 nodes, one of them is miner which creates a new block of information. Then, the confusion mechanism integrates the received data in the blockchain, it gives the users virtual coins and puts the encrypted data in the server. After that, the server stores the users' information and motivates the sensor to collect the information. Their contribution encodes the user information using Confusion Mechanism Encode Algorithm (CMA-E) and hashes the blockchain data by Merkle tree algorithm. They created an information storage system through android application that records the data by traditional and CMA-E methods, where a large percentage of people used the second method. However, the complexity of the Merkle tree algorithm is expensive Tn = O(3n). The encoding algorithm is not strong (it can be broken) since it relies on symmetric cryptography techniques.

Cebe *et al.* [142] create a framework based on the blockchain technology for the forensics of the accident vehicles, it is composed of a forensic daemon inside the vehicle which receives the information from the Event Data Recorders (EDR) and broadcasts Basic Safety Messages (BSM). The forensic daemon publishes the EDR and BSM to the insurance company and the car manufacturers, these latter collect those data to analysis its. The framework does not focus on the types of wireless communication technologies that require high data transmission speed and protection.

Jordi *et al.* [143] achieved an access control framework through LISP control plane and the blockchain implementation (Hyperledger Fabric [1]). Its architecture based on three layers, the first layer is the policies defined by the administrator, that grants the users to access the resources, the second layer is the blockchain which stores all users, companies, and policies; and the third layer is the network which is a set of users, resources, protocols that achieve the access operations (requests-responses). The idea was tested on experiment and verified in terms of scalability and

[1] an open-source implementation of a permissioned blockchain

network latency. On the other hand, its contribution does not concentrate or lack of validation users, also, the structure of block is very basic.

Islam *et al.* [144] enhanced the IoT system by a permissioned blockchain which is consisted on the access control model. The latter is implemented in Hyperledger Fabric which is called Attribute Based Access Control (ABAC). Its proposition collects all of : 1) Actors which are the resource provider and the requester, 2) Components that are a local IoT network and the blockchain , and 3) Resource access process by the requester. With the tested system, they adjusted the values which serve its experiment. The result showed that, the access request of its access control system is faster compared to the public blockchain. On the other hand, the latency increases by increasing the number of attributes in the policy.

The goal of Novo [145] is to propose a decentralized access control system for the IoT devices by using the blockchain technology. The system is composed of WSNs, Managers are responsible for the access control permissions, Agent node deploys the smart contract, smart contract contains all the operations allowed in the access management system. The blockchain network which can be readable from all but only written by the private nodes and Management Hubs that are interfaces which translate the CoAP message received from IoT devices. He evaluated the overall delay of the architecture when including the management hub nodes.The performance of the IoT device is acceptable, but the solution had a waiting issue of the blockchain network to release access control information.

5.3 Blockchain Concepts for Smart Cities

Smart City components (buildings, government, healthcare,) are unified by unique information system, the latter is based on smart objects that differ in their degree of sensitivity, some of them are less, average and highly privacy, for example, at a smart zone, the fixed phone is a public tool, while the personal information server is more private. In addition, the position of users can determine the accessibility of these objects, for example the factory administrator has the authority to access workers' personal information while other workers are denied. Tasks issued by the users play a major role in setting priorities, even if the users 'positions differ, for example, the ordinary user who wants to raise the level of computer protection has priority over the administrator who wants to read information of low importance that can be accessed later

It is known that the digital world is threatened by attacks carried out by hackers, criminals, government agencies, and terrorists [248]. The absence or weakness of access policies may cost the organization (government, economic, education, etc.) heavy losses. However, the policies implemented by the companies are not effective enough because they focus on one aspect which is the employees [**int_2**]. For example, Russian hackers gain access to the servers of government agencies and employees, in addition to the national security threats, the United States of America has spent billions of dollars to address this problem [249].

The blockchain [250] is a digital technology, which was exploited in 2008 by an unknown person, its pseudonym is Satoshi Nakamoto to create the Bitcoin currency. This technology depends on decentralization, meaning that all the parties included in the network have the right to see the content of the information stored in the blockchain, and they also have the right to validate or reject the operations. The blockchain is difficult to falsify due to its copies are distributed to all members of the network, the mining operations need a period of time for each new block, and all blocks are related to each other using hash technology, so, the modification in one block requires a modification of the owned blockchains and all distributed blockchains on the network, but this operation is difficult to achieve. These features guarantee to the users the transparency and the integrity of data.

5.3.1 Hash Function

The hash is a code of fixed size, and any information has its hash through applying a set of arithmetic operations. It is characterized by:

- **The arbitrary message size:** It applies to information of any size.
- **The length of the output is fixed:** The hash size is fixed regardless of the size of the input data.
- **Efficiency:** The calculation process is easy and does not cost much resources.
- **Collision resistance:** It is impossible to find the inputs x and y when $Hash(x) = Hash(y)$.
- **Preimage :** For any input x, the generated output h cannot be found, $Hash(x) = h$.

- **Second-Preimage :** For an input x and its hash $Hash(x)$, the input y cannot be defined if its hash is given $Hash(y)$ and equals the first hash , where, $Hash(x) = Hash(y)$.

Many proposed hash algorithms have been improved to achieve a solid one. Table 5.1 [251] represents the most used algorithms and the difference between their proprieties including block size, word size, output size, the number of rounds and logical operations.

Properties	**Name of Algorithm**				
	MD5	**RIPEMD -160**	**SHA-1**	**SHA-2256/ 512**	**SHA-3256/ 512**
Block Size	512 bits	512 bits	512 bits	512/ 1024 bits	1088/ 576 bits
Word Size	32 bits	32 bits	32 bits	32/64 bits	320/ 320 bits
Output Size	128 bits	160 bits	160 bits	256/ 512 bits	1600/ 1600 bits
Rounds	18	80	80	64/80	24/24

TABLE 5.1: Comparison between the hash functions [251].

The secure hash algorithms are threatened by many attacks that can exploit their vulnerabilities. Table 5.2 [251] shows the possible cryptography attacks that can break the security of hash functions. There are other contributions that aim to prevent or reduce their weaknesses such as [252–255].

Algorithm		**Type of attacks**	**Complexity**
MD5		Collision	2^{39}
		Fast Collision	2^{18}
RIPEM-160		Collision	2^{67}
		Preimage	$2^{158.91}$
SHA-1		Collision	$< 2^{69}$
		Collision	2^{61}
		Freestart Collision	-
SHA-2	256	Preimage	$2^{255.5}$
	512	Preimage	$2^{511.2}$
SHA-3	256	Practical Collision and near-Collision	-
	512	Possibility first Collision	-

TABLE 5.2: The vulnerabilities of the hash functions [251].

5.3.2 RSA Cryptography Algorithm

There are two types of cryptography, "symmetric" and "asymmetric". The first one bases on a single key, that is used to encrypt and decrypt the information, while the asymmetric function uses two keys, the public and the private key. The public key encrypts the data and the private key decodes it (vice versa). This last type of cryptography is more secure because the private key is propertied by the owner and is not distributed in the network, unlike the other which is known by the all users. RSA is an asymmetric algorithm, fast and high encryption ratio [256]. RSA algorithm passes by five steps to generate its keys:

1. Choose two prime numbers p and q.
2. Calculate n where, $n = p \times q$.
3. Calculate $\lambda(n)$ (Carmichael's totient function), where $\lambda(n) = (p-1)(q-1)$.
4. Choose an integer e strictly less than $\lambda(n)$, where, $PGCD(\lambda(n), e) = 1$.
5. Compute d, as $d \equiv e^{-1}(mod\lambda(n))$.

The RSA public key (e,n) encrypts the data $\mathbb{M}$, and the RSA private key (d,n) decodes the encrypted data $\mathbb{M}'$, as follows.

- $\mathbb{M}' = \mathbb{M}^e Mod\, n$, and
- $\mathbb{M} = \mathbb{M}'^d Mod\, n$.

5.3.3 Blockchain

It is a series of blocks (Figure 5.1) where each block contains at least: the information to be stored, its hash and the hash of the previous block. All users spread on the distributed network have the same blockchain. If a user wants to include an information in his blockchain, this latter will be verified by comparing it with all the other distributed blockchains. If the new block is accepted through at least 51% of users, this new block will be distributed over the network level and stored in all other blockchains. In the case where, the user is a malicious and he tampers with his blockchain to serve its interest, other parties will notice the change and the false information will not be included. So the blockchain technology is based on transparency and does not depend on a trusted third party which manages the processes.

Other type of blockchain named a *Smart Contract*, which is a set of conditions agreed upon by all network users, it is applied automatically if achieved, e.g, with banking transactions, the smart contract can contain a condition saying that if a user sends an amount of money to another user without delay in the deadline, the sender will benefit from a 1% bonus, the process will be applied automatically and with everyone's consent.

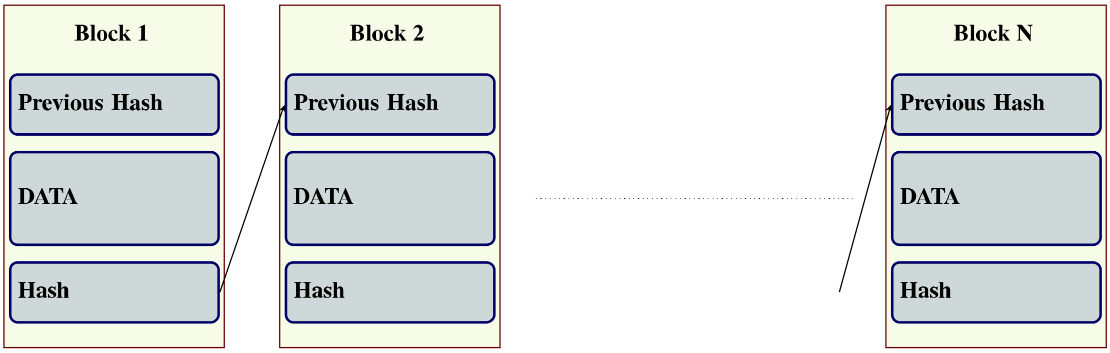


FIGURE 5.1: Basic Blockchain Structure.

5.4 Framework

A smart city has different types of information/data that can change the structure of blockchain, e.g., measurement of sensor buildings, buying and selling operations, police reports, etc. First, we show the deployed blockchain structure. Fig.5.2 represents our structure that fits with a smart city need, and it is is composed of six fields.

1. **Previous Hash:** It is a copy of the previous block hash, as for the genesis block is distinguished by zero.

2. **Data:** Its form depends on its domain of use (e.g., WSN information, worker's personal information, etc.). Data can be readable from all network users, otherwise, the user encrypts its clear data by its RSA public key. Consequently, he should be the only one who can decrypt the message.

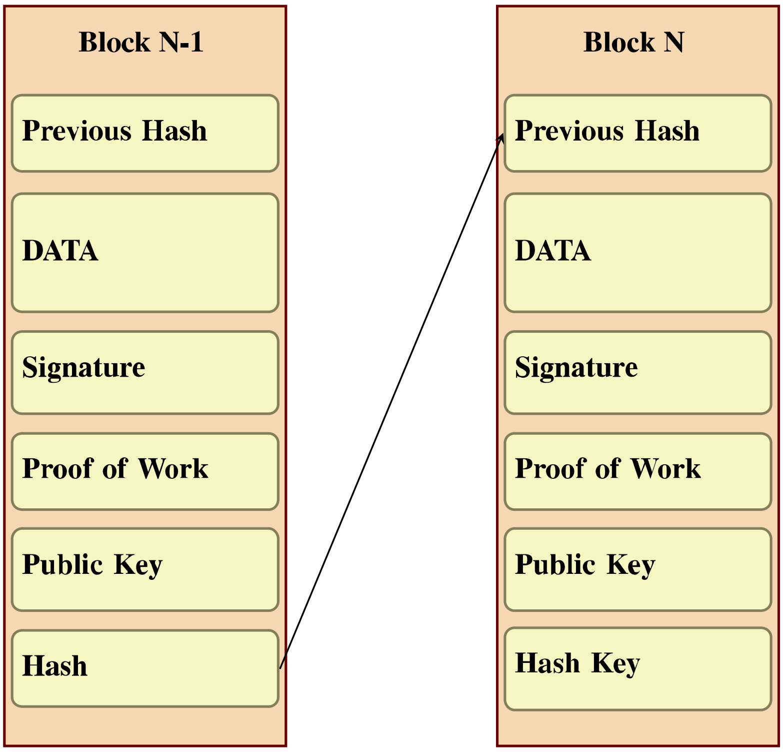


FIGURE 5.2: Blockchain Structure.

3. **Signature:** The data privacy guarantees that its owner is the only one who created this block. This condition is achieved through the digital signature, where, it is a digital fingerprint that confirms the identity of the user. The digital signature $\mathbb{S}$ is produced through encrypting the hash $\mathbb{H}$ of the block by the RSA private key (d,n), where $\mathbb{S} = \mathbb{H}^d \mod n$. To validate the authentication, the decryption of signature by RSA public key (e,n) must equal the hash of block, where, $\mathbb{H} = \mathbb{S}^e \mod n$.

4. **Proof of Work:** It is a value used to create a hash that satisfies a pre-existing condition. It is difficult to find this value in some conditions due to the many generated possibilities. In this case, miner tools are characterized by power-full processors, they have the ability to generate the required hash, the main role to use $Proof of Work$ is to reduce the number of attackers. Of course, the degree of difficulty of the condition is related to the sensitivity of the information. In some information of less importance, this part can be excluded. For example, what is the value $Proof of Work$ for a resulting hash starts with 72 zeros? The hashing process must be calculated 2^{71} times, and a normal computer takes thousands of

years to find this hash.

5. **Public Key:** The approach consists of RSA public key, it is better if its size is 2048 bits or 4096 bits (high-strength key, very high-strength key respectively) according to the sensitivity of information. The public key has two roles, encrypting personal data and checking the validity of the signature included in the block by other users.

6. **Data Hash:** The hash of data is generated by Algorithm 5 where it uses SHA-1, SHA-2, SHA-3 and SHA-5 to prevent the vulnerabilities of each one. It hashes the hash of a new block with the hash of the last block, and the obtained hash will be hashed with the hash of the block before the last, etc. The hash operation will be repeated ten times, except when the size of the the blockchain is less than ten blocks, where, the process will be repeated with the same number of blocks.

Algorithm 5: Hash Blockchain Algorithm.

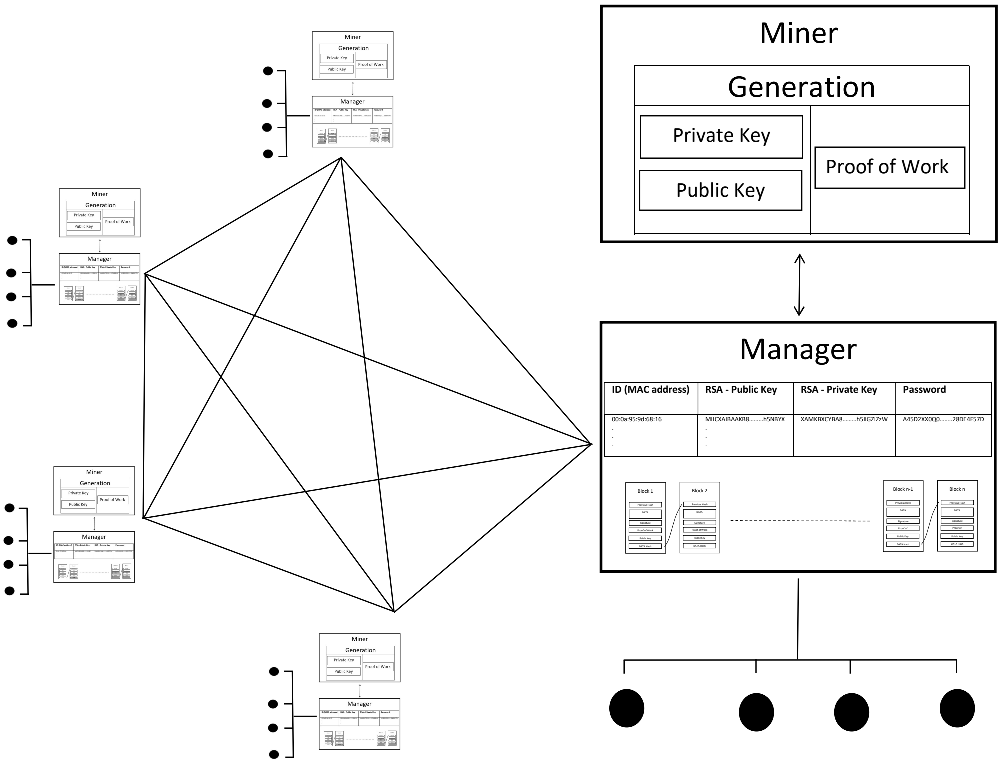
```
$Hash \leftarrow SHA5(SHA3(SHA2(SHA1(New\_DATA))))$
if $NB >= 10$ then
    $n \leftarrow 9$    // NB is the size of the Blockchain.  n+1 is the number of the
      previous block that will be hashed
else
    $n \leftarrow NB - 1$
end
for $i \leftarrow NB$ to $NB - n$ by $-1$ do
    $Hash \leftarrow SHA5(SHA3(SHA2(SHA1(Hash + Hash\_Block[i]))))$
end
return $Hash$
```

5.4.1 Integrity Framework

5.4.1.1 Blockchain Network

The blockchain network included in the smart city is a distributed network, where, each part can connect to the other as illustrated in Figure5.3 by containing the following components.

IoT device: It is an electric device that can *receive*, *send*, *process*, *store*, *encrypt* and *decrypt* data. Mostly, it has low storage, processing and energy consumption capacities. As the case of



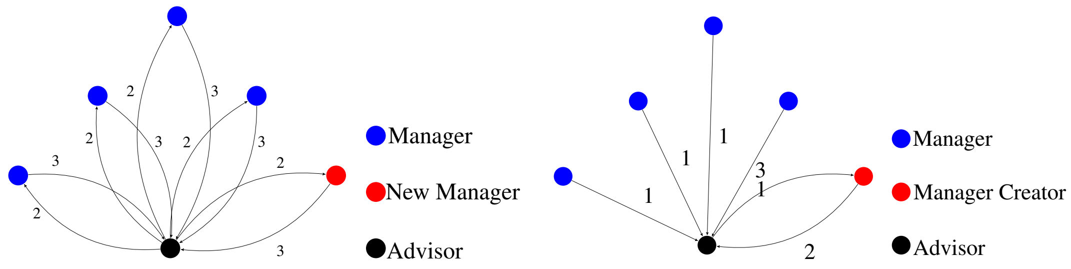
ID (MAC address)	RSA - Public Key	RSA - Private Key	Password
00:0a:95:9d:68:16 . . .	MIICXAIBAAKB8.........h5NBYX . . .	XAMKBXCYBA8.........h5IIGZIZzW	A45D2XX0Q0........28DE4F57D

FIGURE 5.3: Blockchain network.

smartphones, tablets and WSNs, those characteristics do not allow them to store the blockchain in its limited memory.

Manager: It is an unconstrained device that can be under many types of hardware like server, computer or raspberry that featured by high capacities, which provide the IoT devices access to their blockchains. Moreover, the validation and confirmation processes are provided by this component. Since, the MAC address is a unique ID in all the network devices and it can identify 2^{48} objects, so, it is considered as the best identification, especially with the increasing number of IoT devices. Thus, the manager records in its memory the MAC of the registered devices, their RSA keys and their passwords.

Miner: In our proposed network, the mining component has two roles, the first is to create a valid hash through hashing the data and the proof of work together. The generated hash has to respect a predefined condition. The time length of the operation depends on the condition set. All these configurations are to prevent ordinary users from generating random blocks. The second role is to create the RSA keys for each user.



(a) Record New Manager (b) Grant the Mangers Addresses.

FIGURE 5.4: Advisor Tasks.

Advisor: It is the first installed component in the blockchain network, and it has two functions:

A. ***Record New Manager:*** it is summarized in Figure 5.4(a) and it has the operations:

1. Record me and give me the dominant blockchain.
2. Request the blockchain.
3. Get the blockchain.
4. Grant the dominant blockchain.

B. ***Grant the Mangers Addresses:*** all managers that need to validate their new blocks require the addresses of other network managers. This task is applied by the advisor as illustrated in Figure 5.4(b).

1. Store the managers addresses.
2. Request the managers addresses.
3. Provide the addresses.

5.4.1.2 Blockchain Management

It is better if the distance between the devices is close and the connection is wired, also, the communication between them bases to a secure channel such as DTLS protocol, to avoid the Man In the Middle attacks (MIM)[257]. In every home or building can be equipped at least with a manager and a miner. Further, if the IoT device has a high storage and processing capacities, it can work the role of the manager and the miner. This case is more secure due to it avoids the Man

In the Middle attacks (MIM). In the following, we identify three main management operations in the blockchain network.

New Manager. Figure 5.5 illustrates the phases applied when a new manager wants to join a network of the blockchain. First, the new manager contacts the advisor, this letter records its address, then, it extracts the dominant blockchain from the other managers. Finally, the advisor provides the blockchain to the new manager.

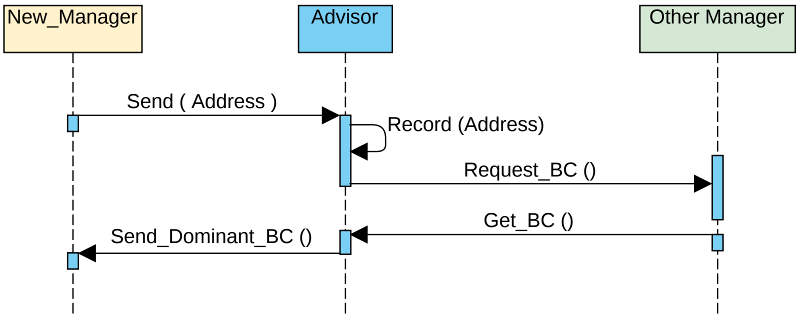


FIGURE 5.5: First New Manager Processes.

User registration. As shown in the sequence diagram of Figure 5.6, the IoT device sends a register request to the manager, that checks the existence of the device in its memory. If this operation is a first inscription, the manager requests the miner about the public and the private key. Then, the miner generates a random pair of keys for the new device. The manager records this pair of keys with the ID (MAC address) of the subscribed device, and it gives a password through hashing the private key. Finally, it provides the password and a message of success to the IoT device.

Add a new block with a secure data. Figure 5.7 illustrates the processes applied when the device wants to share a new data in the network. First the manager authenticates the device, if the it is registered previously, manager grants the access to the IoT device, otherwise the session will be stopped. The authenticated IoT device adds its data in the manager. Then, the latter requests the advisor about the addresses of the managers checker, and after getting addresses, the manager prepares the new block through encrypting the received data with the public key. Consequently, the manager requests the hash from the miner, after the creation of the hash, the manager creates a new block through the information mentioned previously (Figure 5.2). It contacts the managers which compare their blockchains with its blockchain and test the correctness of the new block

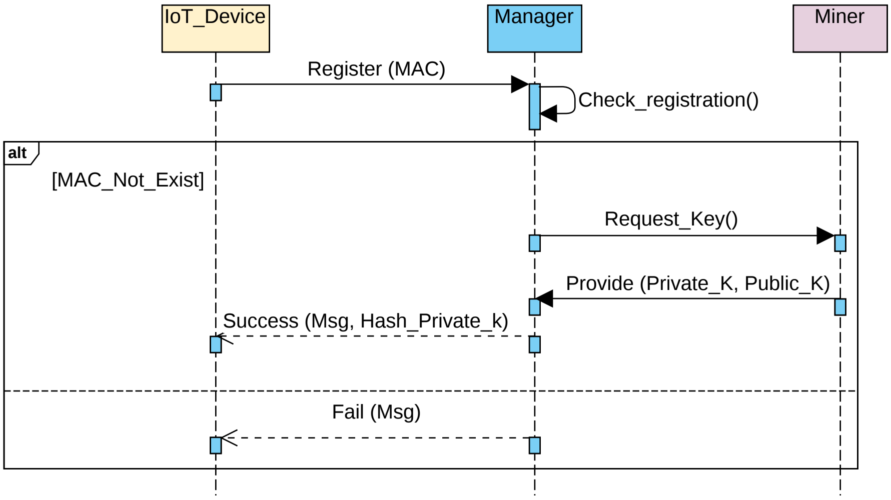


FIGURE 5.6: Registration operation in Manager.

information through checking the device signature by the public key. Also, it verifies if the generated hash from the concatenation of data and proof of work respects the condition defined in the miner. If the device operation is legitimate, the manager attributes all the network managers the new created block, else, the blockchain does not match more than 51% of devices, or the new block contains wrong information. So, the new creation process will be canceled.

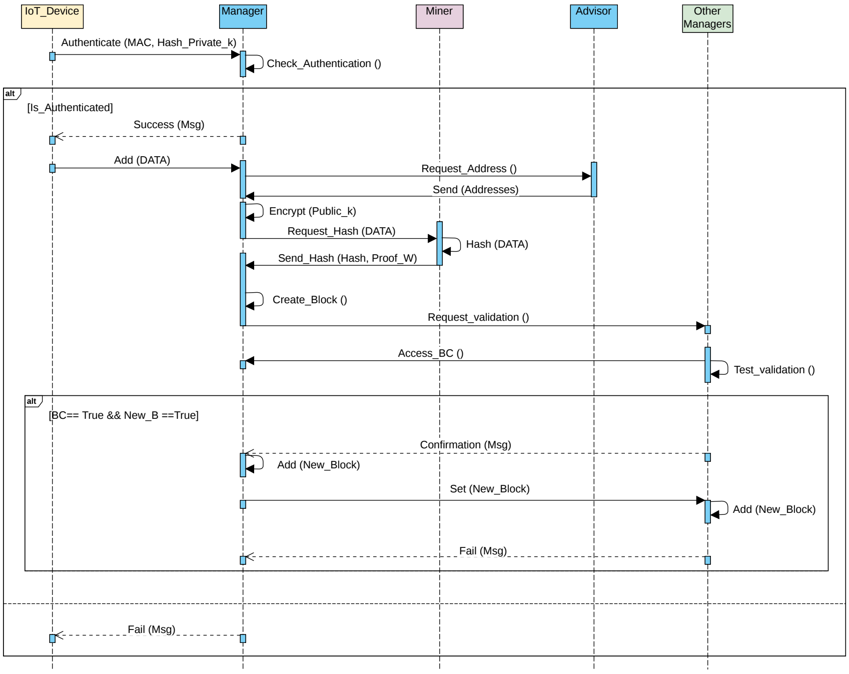


FIGURE 5.7: Add new block with a secure data.

5.4.1.3 The dominance of fraud

Our proposed blockchain network depends on the dominant blockchain in the network. This concept may impose a weakness when the malicious users dominate the majority of the network (or more then 50% malicious). The attackers will participate a single malicious blockchain that serves their interests, causing a loss of network reliability. This risk occurs in two cases, when spreading malicious managers in the network, or when hacking managers.

We propose **V**alidation through **C**onfidence - **A**lgorithm (VCA) 6 against this type of threat. It should be installed in all the managers of network before the attacks occur.The algorithm consists of the "confidences criteria variable" given to the managers. This variable is increasing if the verification processes are correct. The variable will be converted into ranks in order to classify it with the others manager. (e.g. Table.5.3).

Manager	**Confidence Criteria**	**Rank**
M1	100	A
M2	97	A
...	...	...
M50	80	B
...	...	...

TABLE 5.3: Classify the Managers.

VCA defines the interesting ranks and their ratios of managers which will test the new block, the chosen random managers will be recorded in a table. It passes the new block to the managers in order to count the managers which accept this block. If the ratio of the acceptation decision equals the ratio of rejecting decision, the algorithm will extract a new random population. If the ratio of the acceptation decision is the greater, the new block will be shared on the network to add it with all managers, in addition, it increases the confidence criteria of the managers which accept the new block, then, it deletes the addresses of the managers which reject it from the advisor and it initializes their confidence criteria. Otherwise, if the ratio of the rejecting decision is the major, the new block will be ignored, in addition, it increases the confidence criteria of the managers which reject the new block and it deletes the addresses of the managers which accept it from the advisor and it initializes their confidence criteria.

In our proposition, VCA can decrease the confidence criteria of the managers which have minorities decision instead of deleting them from the network (to reduce the punishment). Also, we do not install the VCA in the advisor due to:

- Make the blockchain network distributed.
- Maintaining the transparency concept where the users are the owners.
- The damage of the advisor by an attack (e.g., Distributed Denial-of-Service (DDoS) [258]) cause the absence of the VCA service.

Algorithm 6: Validation through the Confidence Algorithm (VCA).

```
Define the rank and its ratio                // e.g: Rank_A ← 60% ; Rank_B ← 20%
do
    for $i \leftarrow 1$ to $N$ do
        Confidence [i] ← Random(Rank)        // N: The number of the nodes chosen
        /* Fill the confidence table by random nodes */
    end
    for $i \leftarrow 1$ to $N$ do
        Res ← Block_accept(Confidence [i], NewBlock)
        if $Res == True$ then
            decision_Accept ++               // Count the nodes which accept the new block
        end
    end
while $decision\_Accept\_ratio == 50$
if $decision\_Accept\_ratio > 50$ then
    Add_Block(NewBlock)
    Increase_Node()  // Increase the confidence criteria of the nodes which accept the new block
    Delete_Node()                            // Delete nodes which reject the new block
else
    Increase_Node()  // Increase the confidence criteria of the nodes which reject the new block
    Delete_Node()                            // Delete nodes which accept the new block
end
```

5.4.1.4 Verification time

The continual increase in the number of nodes and blockchain size in the network causes a decrease in the speed of sharing blocks. Equation 5.1 calculates the time spent ($\mathbb{T}$) in order to check the blockchain of the manager created by others managers, where $\mathbb{N}$ is the number of managers, $\mathbb{S}$ is the size of the blockchain and $\mathbb{B}$ is the time spent to check one block.

$$\mathbb{T} = \mathbb{N} \times \mathbb{S} \times \mathbb{B} \tag{5.1}$$

To solve this problem, we determine the ratio of managers checkers τ_1 and the ratio of the blocks which will be verified τ_2. We note that the blocks that must be verified are the last blocks of the blockchains for quick access to them. The new time $\top$ will be calculated through Equation 5.2. We substitute Equation 5.1 into Equation 5.2, and the final equation will be Equation 5.3.

$$\top = \tau_1 \times \tau_2 \times \mathbb{N} \times \mathbb{S} \times \mathbb{B} \tag{5.2}$$

$$\top = \tau_1 \times \tau_2 \times \mathbb{T} \tag{5.3}$$

The curve presented in Figure 5.8 displays the time spent $\top$ in terms of the ratios τ_1 and τ_2, considering that the original time $\mathbb{T}$ is one minute. Note that the smaller the two ratios τ_1 and τ_2, the smaller the time it takes to verify the blockchain $\top$. However, too much decrease in the two ratios may cause the network to lose its robustness.

5.4.1.5 Theft the private key

The integrity of information and privacy of users are depended on the private and the public keys generated to any device. If the private keys will be attacked by the sniffing attack, the blockchain network will lose these features. The solution is to create a secure channel between the miner (generator), the manager (decrypt and sign) and the IoT devices (reader and writer). Table 5.4 shows the possible secure network protocols which can be used to protect the end to end communications. We rely on the following cretiria in our framework to select a secure channel.

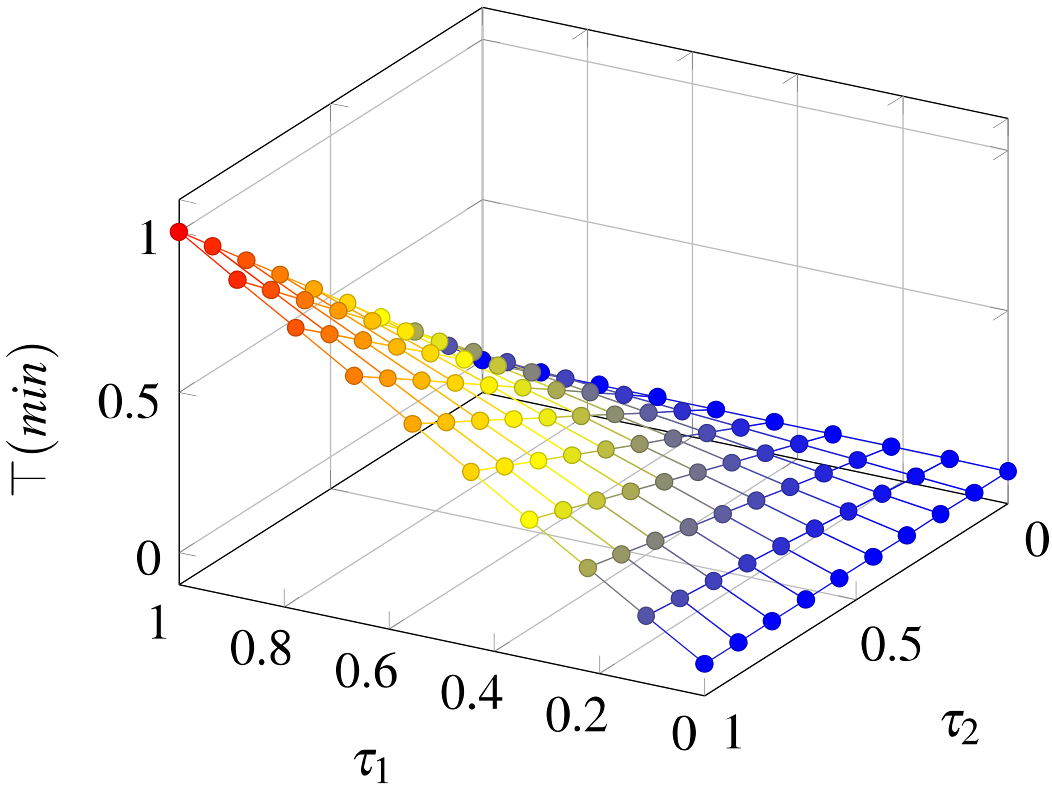


FIGURE 5.8: Time taken in terms of the ratios τ_1 and τ_2.

- **Implementation of Software:** the secure protocol should support the used layer in the communication software.

- **Capacity of Devices:** certain devices have a limited memory and CPU, which do not support the large frame size of the communication protocols.

- **Energy Consumption:** the protocols which have a large size and expensive cryptography algorithms cause a high energy consumption, so, they can not fit some constrained devices.

- **Type of Threat:** the type of network attacks (e.g., sniffing, spoofing, tampering, etc.) determines the encryption algorithm used that protocols support.

5.4.2 Access Control Management

Our access control system named **Subject-Object-Task System** ($\mathbb{SOT}-\mathbb{S}$) consists on three entities, Subject $\mathbb{S}$, Object $\mathbb{O}$ and Task $\mathbb{T}$, where:

Protocol	Layer	Size	Cryptography
IEEE 802.15.4	Physical layer	127 bytes	AES (Advanced Encryption Standard) with a 128b key length
IPsec/VPN	Network layer	136 bytes with tunnel mode encrypting	Triple DES or AES
Transport Layer Security (TLS)	Transport layer	16 KB	AES, Camellia or ARIA
Datagram Transport Layer Security (DTLS)	Transport layer	DTLS.v3, in theory up to 2ˆ24-1 bytes, in practice many kilobytes	AEAD which is based on AES
Secure Shell (SSH)	Transport layer	35000 KB or less	AES, Blowfish, 3DES, CAST128, and Arcfour

TABLE 5.4: Characteristics of secure protocols.

- **Subject $\mathbb{S}$:** is a human, a software, or a machine which gives the commands to the objects O in order to achieve a tasks T.
- **Object $\mathbb{O}$:** Applies the tasks T after receiving commands from the subjects S.
- **Task $\mathbb{T}$:** is reading or updating actions applying from the object O to achieve the subject S goals.

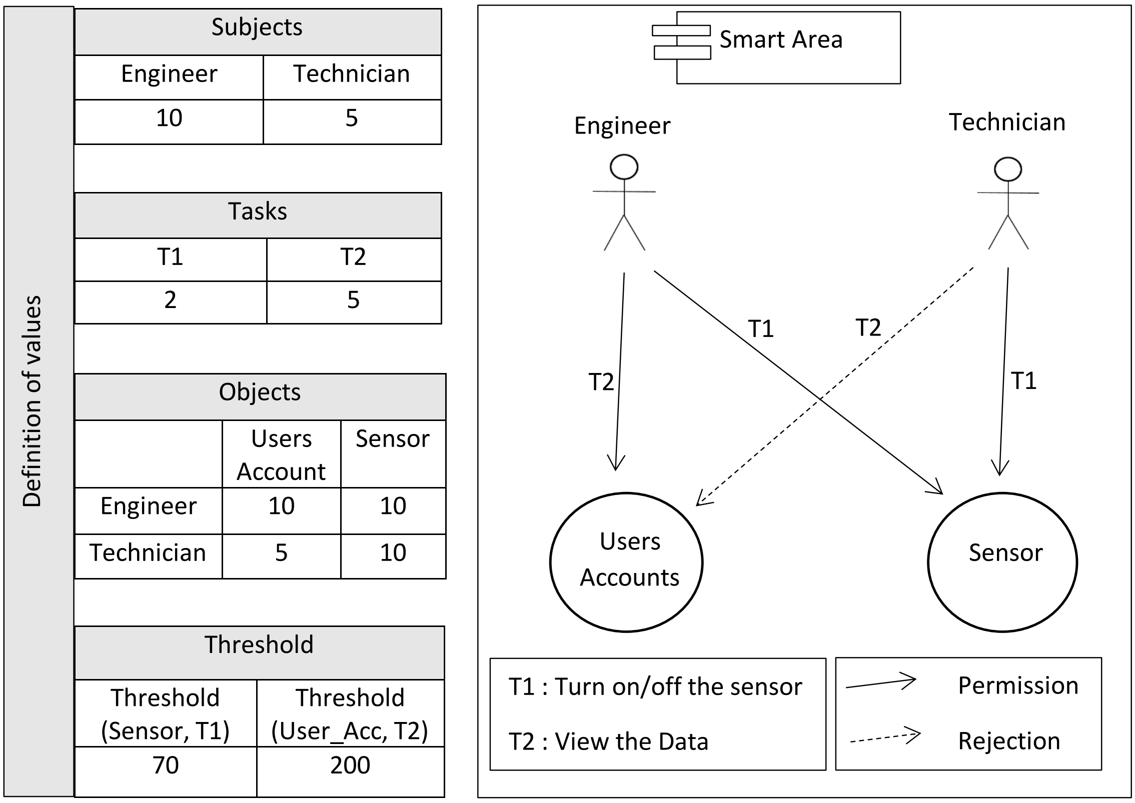
$\mathbb{SOT}-\mathbb{S}$ achieves two issues, the first is the "Authorisation" which gives the subject S permission/rejection to the object O for a specific task T. The second issue is setting priorities for subjects S to gain access to the object O. Both issues consist on common formula, Eq. 5.4.

$$\mathbb{A}(i,j,k) = \mathbb{S}_i \times \mathbb{O}(\mathbb{O}_k,\mathbb{S}_i) \times \mathbb{T}_j \tag{5.4}$$

Eq. 5.4 calculates the value of access $\mathbb{A}(i,j,k)$ by multiplying the subject value $\mathbb{S}_i$ in the network by its task value $\mathbb{T}_j$ and the relationship of the target object to the subject $\mathbb{O}(\mathbb{O}_k, \mathbb{S}_i)$.

Authorisation issue. Some subjects S which have low values, and want to access to a sensitive object O (have high value) with low task value, they will be rejected due to the low value calculated by the Eq. 5.4, and vice versa with the subjects S and tasks T which have high values. This correct logical principle will be applied through defining thresholds Threshold($\mathbb{O}_k$, $\mathbb{T}_j$) to determine the value needed to access the object O by the task T. If $\mathbb{A}(i,j,k) \geq$Threshold($\mathbb{O}_k$, $\mathbb{T}_j$) is true, the subject S_i has the access, and vice versa (Algorithm 7).

Example. Figure 5.9 presents the correctness of this principle. The smart area has two subjects "Engineer" and "Technician", and two objects "Users accounts" and "Sensor". Both subjects want access to the objects by the tasks T_1 (Turn on/off the sensor) and T_2 (view the data). The parameters values on the smart area are shown in rows (Figure 5.9). Table 5.5 shows the requests access that can be authorized or rejected through applying the Eq. 5.4. Note that both requests are authorized, except the last one, because in this latter the Technician has a low value for accessing a critical object as "Users accounts".



Definition of values

Subjects	
Engineer	Technician
10	5

Tasks	
T1	T2
2	5

Objects		
	Users Account	Sensor
Engineer	10	10
Technician	5	10

Threshold	
Threshold (Sensor, T1)	Threshold (User_Acc, T2)
70	200

FIGURE 5.9: Example of Permission and Rejection Cases

Request	Calculation $\mathbb{A}(i,j,k)$	Response
Engineer turns on/off the sensor	Engineer $\times$ $\mathbb{T}_1$ $\times$ $\mathbb{O}$(Sensor,Engineer) = 10 $\times$ 2 $\times$ 10 = 200 $\Rightarrow$ $\mathbb{A}(i,j,k) \geq$ Threshold (Sensor, $\mathbb{T}_1$)	✓
Technician turns on/off the sensor	Technician $\times$ $\mathbb{T}_1$ $\times$ $\mathbb{O}$(Sensor,Technician) = 5 $\times$ 2 $\times$ 10 = 100 $\Rightarrow$ $\mathbb{A}(i,j,k) \geq$ Threshold (Sensor, $\mathbb{T}_1$)	✓
Engineer views the users accounts	Engineer $\times$ $\mathbb{T}_2$ $\times$ $\mathbb{O}$(U_Account,Engineer) = 10 $\times$ 5 $\times$ 10 = 500 $\Rightarrow$ $\mathbb{A}(i,j,k) \geq$ Threshold (U_Account, $\mathbb{T}_2$)	✓
Technician views the users accounts	Technician $\times$ $\mathbb{T}_2$ $\times$ $\mathbb{O}$(U_Account,Technician) = 5 $\times$ 5 $\times$ 5 = 125 $\Rightarrow$ $\mathbb{A}(i,j,k) <$ Threshold (U_Account, $\mathbb{T}_2$)	✗

TABLE 5.5: Permission/Rejection the requests access cases.

Priorities issue. Whenever the value obtained from Eq. 5.4 for a subject S which uses the object O in a task T is greater compared to other subjects which want to use the same object O, the priority will be given to the subject S through Algorithm 8. As example, Figure 5.10 and Table 5.6 shows the correctness of this principle. The rank of the requested access in the smart areas is related to the affect of their parameters ($\mathbb{S}$,$\mathbb{O}$ and $\mathbb{T}$). In case$_1$, the priority was given to the request $\mathbb{A}_1$ since the Engineer has a greater value compared to the Technician$_1$. In case$_2$, although the Technician$_1$ has small value compared to the Engineer, but his task is more important, so Technician$_1$ has the priority. In case$_3$, although Technician$_1$ and Technician$_2$ have the same value and they want to access to the same object (Sensor$_2$) with the same task ($\mathbb{T}_2$), but the priority will given to the Technician$_2$ because Sensor$_2$ is under the responsibility of Technician$_2$.

Algorithm 7: Permission Access policy

```
if $A(i,j,k) >= Threshold(O_k,T_i)$ then
    return $True$
else
    return $False$
end
```

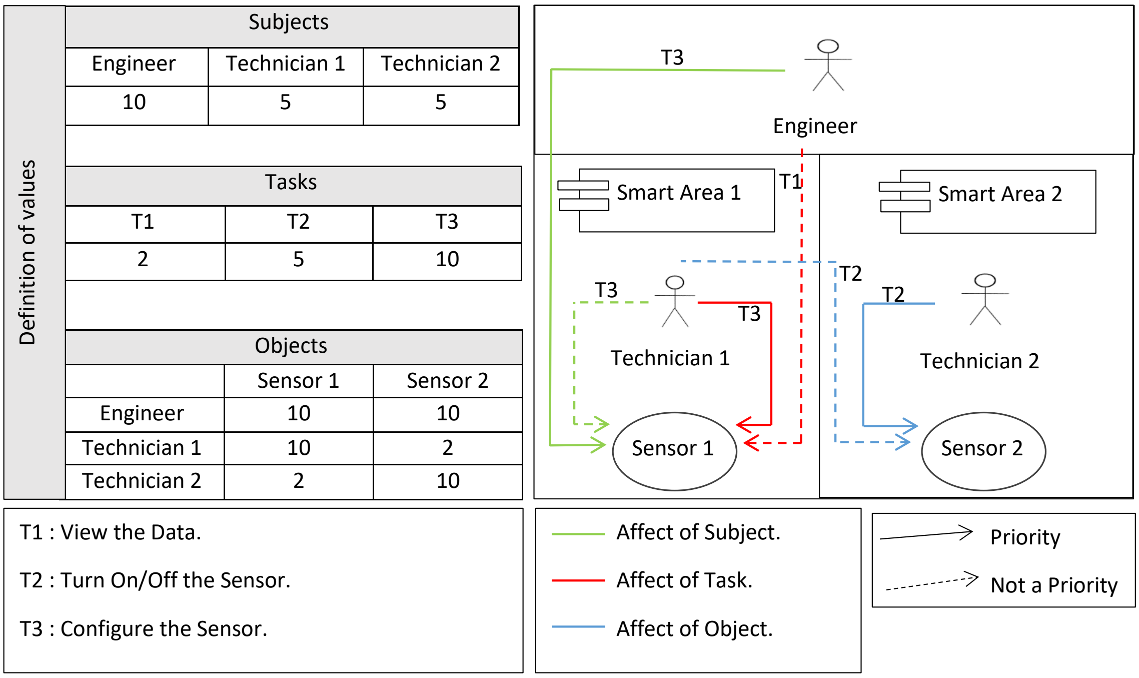
Algorithm 8: Subjects Access through Priorities.

```
Structure $Access$
    $Subject, Object, Task$
$Access : Tab\_access[]$
$Tab\_access[] \leftarrow Get\_Access()$    // Fill the parameters values of all access requests
for $i \leftarrow 1$ to $Tab\_access.Length$ do
    $A \leftarrow Calc\_A\_V(Tab\_access[i])$    // Calc_A_V(): Calculate the Access Value
    if $A > MAX$ then
        $MAX \leftarrow A$
        $MAX_i \leftarrow i$    // Get the index of the subject which has the max priority
    end
end
return $MAX_i$
```

5.4.2.1 Access Control Blockchain

For a better access control management, we consider five types of blockchains, the difference among them is at the type of the *Data* (see. Figure 5.11):

- **Subject-Blockchain:** Every new subject which joins the network is registered in the blockchain by creating his own block, that contains its ID, position, value and date of creation.
- **Object-Blockchain:** Every object should be valued for network subject through determining in each block the following parameters: ID object, ID subject, value and date of creation.
- **Task-Blockchain:** The tasks that the users perform are coded and valued by the parameters: ID Task, value and date of creation.



Definition of values

Subjects		
Engineer	Technician 1	Technician 2
10	5	5

Tasks		
T1	T2	T3
2	5	10

Objects		
	Sensor 1	Sensor 2
Engineer	10	10
Technician 1	10	2
Technician 2	2	10

T1 : View the Data.

T2 : Turn On/Off the Sensor.

T3 : Configure the Sensor.

FIGURE 5.10: Example of Access Control with Priority.

- **Threshold-Blockchain:** Every task applied to an object must equal or exceed a threshold defined on this type of blockchain, that is characterised by: ID Task, ID Object, value and date created.

- **Smart contract:** We have two types of policies (Algorithm 7 and Algorithm 8), they are integrated in this type of blockchain by specifying the parameters: ID Policy, Rules (or policies) and date of creation.

5.4.2.2 $\mathbb{SOT}-\mathbb{S}$ Network

The *Network* distributed over the smart zone, regardless its size (smart factory, smart building, smart city, etc), is composed of four parts: *Advisor*, *Miner*, *Subject* and *Object*. These types are described in a common tuple $Type =< ID,Func,Numb,Comm >$, where:

- *ID*: is a set of unique identities, that reference the components system, such that: $if\ ID \neq \varnothing \wedge id_1 \in ID \Rightarrow \exists! id_1$.

- *Func*: is a set of actions applied by the component through exploitation the inputs *In*, where: $Func = \{Func_1(In_1,..,In_i),...,Func_n(In_1,..,In_i) \mid i,n \in \mathbb{N}\}$.

Affect of	Concurrent Requests	Comparison the Request Access	Response
Subject $\mathbb{S}$ $Case_1$	Both the Engineer and Technician$_1$ wants to configure the Sensor$_1$	$\mathbb{A}_1$ = Engineer × $\mathbb{O}$(Sensor$_1$,Engineer) × $\mathbb{T}_3$= 1000. $\mathbb{A}_2$ = Technician$_1$ × $\mathbb{O}$(Sensor$_1$,Technician$_1$) × $\mathbb{T}_3$=500. $\Rightarrow \mathbb{A}_1 > \mathbb{A}_2$	The Engineer has the priority
Task $\mathbb{T}$ $Case_2$	The Engineer wants to view the data collected from the Sensor$_1$, and the Technician$_1$ wants to configure the same sensor	$\mathbb{A}_1$ = Engineer × $\mathbb{O}$(Sensor$_1$,Engineer) × $\mathbb{T}_1$= 200. $\mathbb{A}_2$ = Technician$_1$ × $\mathbb{O}$(Sensor$_1$,Technician$_1$) × $\mathbb{T}_3$=500. $\Rightarrow \mathbb{A}_1 < \mathbb{A}_2$	The Technician$_1$ has the priority
Object $\mathbb{O}$ $Case_3$	Both the Technician$_1$ and Technician$_2$ want to turn on/off the Sensor$_2$	$\mathbb{A}_1$ = Technician$_1$ × $\mathbb{O}$(Sensor$_2$,Technician$_1$) × $\mathbb{T}_2$= 50. $\mathbb{A}_2$ = Technician$_2$ × $\mathbb{O}$(Sensor$_2$,Technician$_2$) × $\mathbb{T}_2$=250. $\Rightarrow \mathbb{A}_1 < \mathbb{A}_2$	The Technician$_2$ has the priority

TABLE 5.6: The Affect of parameters ($\mathbb{S}$,$\mathbb{O}$ and $\mathbb{T}$) in determining the priorities.

- *Numb*: it donates the number of components within the network, where: *if* $ID \neq \varnothing \Rightarrow Numb > 0$.
- *Comm*: it is the communication package, that has a set of functions "*Conn*" which allow to *connect* with *n* components, each type of components has a table of size *i*, where: $Comm = \{Conn_1(Type_1[i]),..,Conn_n(Type_n[i]) \mid i,n \in \mathbb{N}\}$.

Advisor. It is a logical representation given by $Advisor = \langle ID_{Ad}, Func_{Ad}, Numb_{Ad}, Comm_{Ad} \rangle$, where:

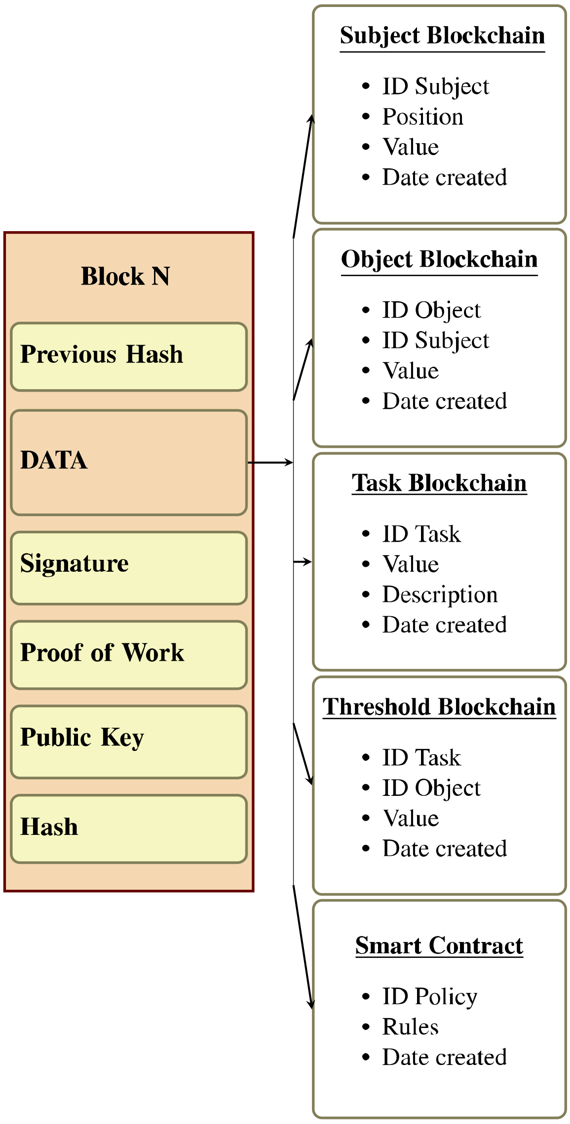


FIGURE 5.11: Types of Blockchain.

- ID_{Ad}: is a set of constant identifications and it is better to be represented by a $MAC\,addresses$, where: $if\ ID_{Ad} \neq \varnothing;\ \exists\ id_1 \in ID_{Ad} \wedge \forall\ id_2 \in ID_{Ad} \Rightarrow id_1 \neq id_2$.

- $Func_{Ad}$: combines all processes, where: $Func_{Ad}$ = $\{\ Send(inf),\ Receive(),\ Record(inf),\ Create\_Block(inf_1,..,inf_n),\ Encrypt(Key,inf),\ Decrypt(Key,inf),\ Sign(Key,Hash)\ \}$.

- $Numb_{Ad}$: The $Network$ should contain only one $Advisor$; where: $if\ Network \neq \varnothing \Rightarrow \exists\ Advisor \mid 1 \leqslant Numb_{Ad} \leqslant 1$.

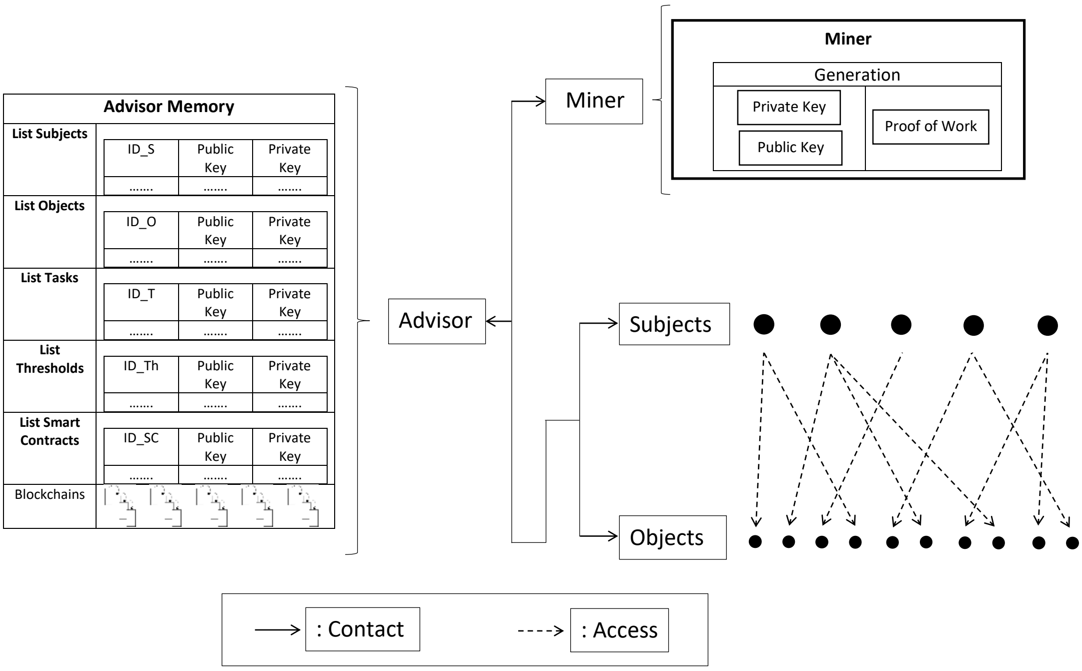


FIGURE 5.12: Blockchain Network.

- $Comm_{Ad}$: establishes the communication with the following types, where: $Comm_{Ad} = \{ Conn(Miner[n]), Conn(Subject[n])\ \}, Conn(Object[n])) \mid n \in \mathbb{N} \wedge n \neq 0\}$.

The behavior of an advisor in the network is summarized as follows:

- Record New Subject: The new network subject contacts the advisor, the latter records its address (Or ID), then it provides it the blockchains.
- Record New Object: When a new object is included in the network, its ID will be stored in the advisor's memory.
- Add New Blocks: All types of blocks (see Figure 5.11) are generated through the advisor. It shares the new block with all subjects in order to update the blockchains.

Subject. As mentioned in Figure 5.13, the subject has two main roles: access to objects and validate the access. The subject that want to access to a specific object must obtain the validation from the subjects network. The latter checks the integrity of its blockchain by comparing its blockchains hash with their own hashes. They check the authorisation issue (Algorithm 7), and checks its priority with another subject connected with the same object (Algorithm 8). If the verification processes return positive results from the majority of subjects (more than 50%), the subject can access to the object, else the subject is denied. A subject is represented by the tuple $Subject = \langle ID_{Su}, Func_{Su}, Numb_{Su}, Comm_{Su} \rangle$, where:

- ID_{Su}: is a set of static identifications proposed to be a $MAC addresses$, where: $if\ ID_{Su} \neq \varnothing;\ \exists\ id_1 \in ID_{Su} \wedge \forall\ id_2 \in ID_{Su} \Rightarrow id_1 \neq id_2$.
- $Func_{Su}$: is a set of operations, where: $Func_{Su} = \{Send(inf), Receive(), Access(Object, Task), Validate\_Access(), Cut\_Access(), Record(inf)\}$.
- $Numb_{Su}$: The $Network$ can be configured by $n\ Subjects$; where: $if\ Network \neq \varnothing \Rightarrow Numb_{Su} \in \mathbb{N}$.
- $Comm_{Su}$: it grants the $Subject$ to connect with the following types, where: $Comm_{Su} = \{Conn(Advisor[1]), Conn(Subject[n]), Conn(Object[n]) \mid n \in \mathbb{N}\}$.

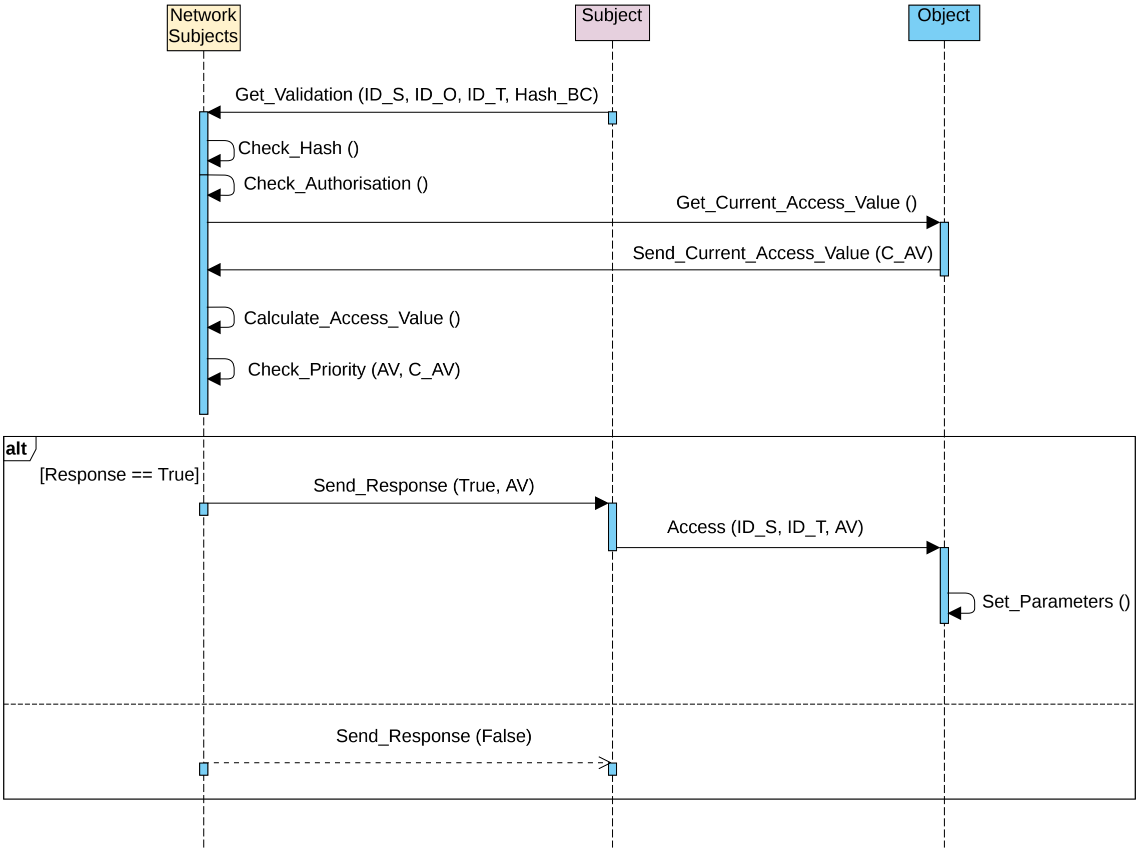


FIGURE 5.13: Access Control Processes.

Object. It is a software or hardware component, accessed by subjects and referenced by ID. With the high increase of IoT devices, it is better to take the MAC address as an identification for the hardware components, due to the large number of identities it provides 2^{48}. It is described by the following formulas: An *Object* is a the tuple $\langle ID_{Ob}, Func_{Ob}, Numb_{Ob}, Comm_{Ob} \rangle$, where:

- ID_{Ob}: is a set of unique identifications suggested to be a $MAC addresses$, where: $if\ ID_{Ob} \neq \varnothing; \exists\ id_1 \in ID_{Ob} \wedge \forall\ id_2 \in ID_{Ob} \Rightarrow id_1 \neq id_2$.
- $Func_{Ob}$: is a set of operations, where: $Func_{Ob} = \{Send(inf), Receive(), \quad Grant\_Access(Subject, Tas$ $Record(inf)\}$.
- $Numb_{Ob}$: The $Network$ can be equipped with an unlimited number of $Objects$; where: $if\ Network \neq \varnothing \Rightarrow Numb_{Ob} \in \mathbb{N}$.
- $Comm_{Ob}$: allows the $Object$ to link with the following components, where: $Comm_{Ob} = \{ Conn(Advisor[1]), Conn(Subject[n]) \mid n \in \mathbb{N}\}$.

Miner. It is mining component characterised by a high processing capacity applying two functions. The first is to generate a hash of the peer (data + proof of work), the hash must respect a predefined condition, where the more difficult is the condition, then the more difficult is the process. The difficulty of condition depends of the sensibility of the data. The second function is to create the private and the public RSA keys for each subject. A Miner is the tuple $\langle ID_{Mi}, Func_{Mi}, Numb_{Mi}, Comm_{Mi} \rangle$; where:

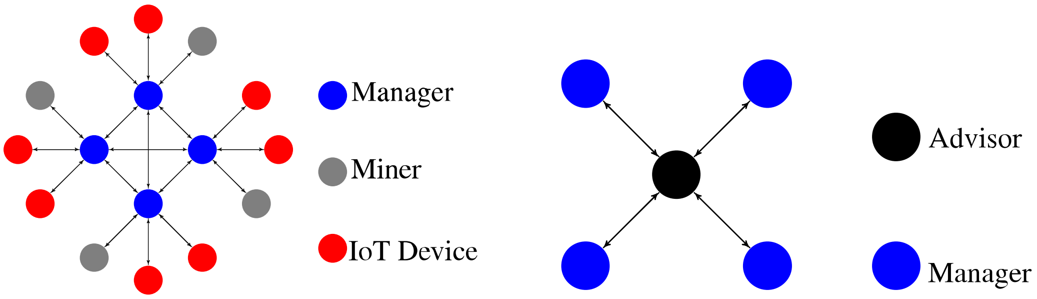
- ID_{Mi}: is a set of constant identifications that we suggest expressing with a $MAC addresses$, where: $if\ ID_{Mi} \neq \varnothing; \exists\ id_1 \in ID_{Mi} \wedge \forall\ id_2 \in ID_{Mi} \Rightarrow id_1 \neq id_2$.
- $Func_{Mi}$: is a collection of operations, where: $Func_{Mi} = \{Send(inf), Receive(), Generate\_Hash(inf), Generate\_Keys()\}$.
- $Numb_{Mi}$: The $Network$ has at least one $Miner$; where: $if\ Network \neq \varnothing \Rightarrow \exists\ Miner \mid Numb_{Mi} \in \mathbb{N} \wedge Numb_{Mi} \neq 0$.
- $Comm_{Mi}$: it allows to connect with the types; where: $Comm_{Mi} = \{Conn(Advisor[1])\}$.

5.5 Experimental Results

5.5.1 Integrity of Information Issue

5.5.1.1 Network Configuration:

This test demonstrates the applicability of the proposition mentioned above (sequence diagrams 5.5, 5.6 and 5.7). The experiment is developed in a JAVA environment by creating a decentralized network composed of four managers related by the advisor (Figure 5.14(b)), where each manager has a miner and two IoT devices (Figure 5.14(a)).



(a) The blockchain topology (IoT Devices, Miners and Managers).

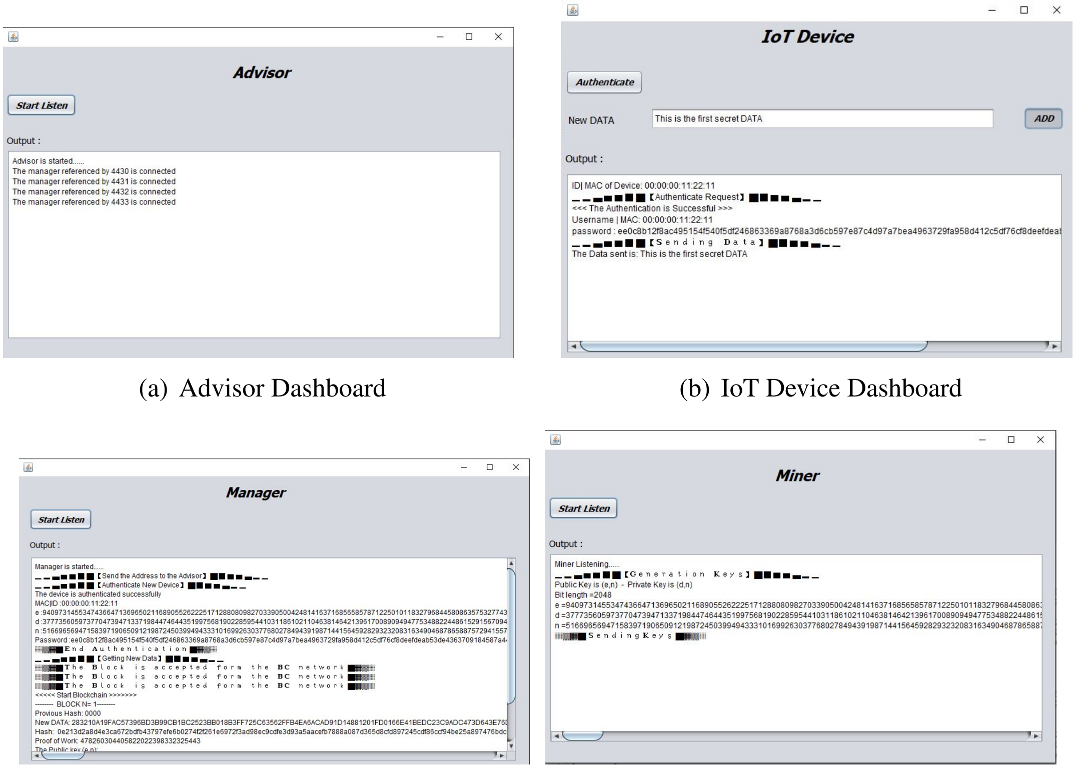
(b) The blockchain topology (Manager & Advisor).

FIGURE 5.14: Topology of the Blockchain Network.

The generated information by the IoT devices is encrypted through their public keys which is provided by the miners, the blockchains of the network are installed in the managers. The P2P communication depends on the sockets. The hash algorithm 5 searches of the proof of work that produces with the data a hash which respects this condition: every generated hash should begin with at least zero. To enhance the integrity of the data and the privacy of the users, the size of the RSA private keys consists of 2048 bits. We applied a test scenario (Fig.5.15), where the managers joined by the advisor to get the dominant blockchain, the IoT devices registered in their mangers, the data was encrypted, validated with the managers, and added in the network blockchains.

5.5.1.2 Integrity Attack

We consider a malicious attacker who changes the data blockchain of one manager in order to create a blockchain which serves his personal interests (Fig. 5.16(a)). As a next step, the damaged



```
Advisor is started......
The manager referenced by 4430 is connected
The manager referenced by 4431 is connected
The manager referenced by 4432 is connected
The manager referenced by 4433 is connected
```

(a) Advisor Dashboard

New DATA: This is the first secret DATA

```
ID| MAC of Device: 00:00:00:11:22:11
【Authenticate Request】
<<< The Authentication is Successful >>>
Username | MAC: 00:00:00:11:22:11
password : ee0c8b12f8ac495154f540f5df246863369a8768a3d6cb597e87c4d97a7bea4963729fa958d412c5df76cf8deefdeat
【Sending Data】
The Data sent is: This is the first secret DATA
```

(b) IoT Device Dashboard

```
Manager is started......
【Send the Address to the Advisor】
【Authenticate New Device】
The device is authenticated successfully
MAC|ID :00:00:00:11:22:11
e :9409731455347436647136965021168905526222517128808098270339050042481416371685658578712250101183279684458086357532774
d :3777356059737704739471337198447464435199756819022859544103118610211046381464213961700890949477534882244861529156709
n :5166965694715839719065091219872450399494333101699263037768027849439198714415645928293232083163490468786588757294155
Password :ee0c8b12f8ac495154f540f5df246863369a8768a3d6cb597e87c4d97a7bea4963729fa958d412c5df76cf8deefdeab53de4363709184587a4
End Authentication
【Getting New Data】
The Block is accepted form the BC network
The Block is accepted form the BC network
The Block is accepted form the BC network
<<<<< Start Blockchain >>>>>>>
-------- BLOCK N= 1--------
Provious Hash: 0000
New DATA: 283210A19FAC57396BD3B99CB1BC2523BB018B3FF725C63562FFB4EA6ACAD91D14881201FD0166E41BEDC23C9ADC473D643E76
Hash:  0e213d2a8d4e3ca672bdfb43797efe6b0274f2f261e6972f3ad98ec9cdfe3d93a5aacefb7888a087d365d8cfd897245cdf86ccf94be25a897476bdc
Proof of Work: 478260304405822022398332325443
The Public key (e,n):
```

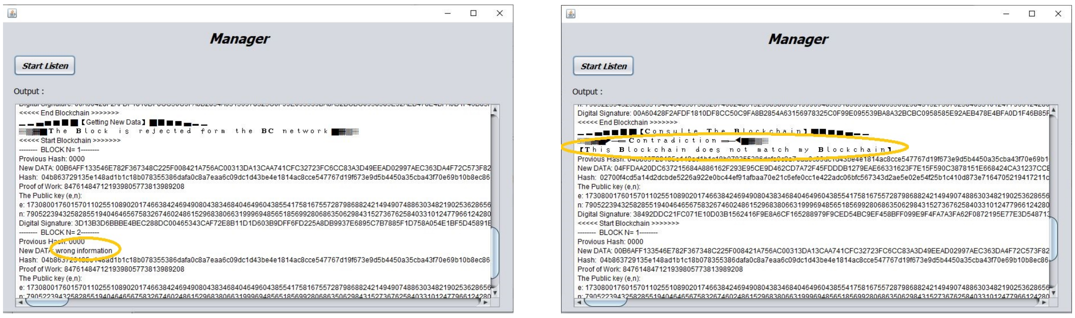
(c) Manager Dashboard

```
Miner Listening......
【Generation Keys】
Public Key is (e,n)  -  Private Key is (d,n)
Bit length =2048
e =9409731455347436647136965021168905526222517128808098270339050042481416371685658578712250101183279684458086
d =3777356059737704739471337198447464435199756819022859544103118610211046381464213961700890949477534882244861
n =5166965694715839719065091219872450399494333101699263037768027849439198714415645928293232083163490468786588
Sending Keys
```

(d) Miner Dashboard

FIGURE 5.15: Registration, authentication and creation block scenarios.

manager receives a request from an IoT device that wants to add its data in the blockchains network. Then, the damaged manager shares the new block with the other managers in order to get the validation from them. Thus, the network managers find the discrepancy in its blockchain with their blockchains. As a result, the new block will be rejected (Figure 5.16(b)).



```
<<<<< End Blockchain >>>>>>>
【Getting New Data】
The Block is rejected form the BC network
<<<<< Start Blockchain >>>>>>>
-------- BLOCK N= 1--------
Provious Hash: 0000
New DATA: 00B6AFF133546E782F367348C225F008421A756AC00313DA13CAA741CFC32723FC6CC83A3D49EEAD02997AEC363DA4F72C573F82
Hash:  04b863729135e148ad1b1c18b078355386dafa0c8a7eaa6c09dc1d43be4e1814ac8cce547767d19f673e9d5b4450a35cba43f70e69b10b8ec86
Proof of Work: 847614847121939805773813989208
The Public key (e,n):
e: 17308001760157011025510890201746638424694908043834684046496043855417581675572879868824214949074886303482190253628656
n: 79052239432582855194046465675832674602486152968380663199969485651856992806863506298431527367625840331012477966124280
Digital Signature: 3D13B3D6BBBE4BEC288DC00465343CAF72E8B11D1D603B9DFF6FD225A8DB9937E6895C7B7885F1D758A054E1BF5D45891E
-------- BLOCK N= 2--------
Provious Hash: 0000
New DATA: wrong information
Hash:  04b863729135e148ad1b1c18b078355386dafa0c8a7eaa6c09dc1d43be4e1814ac8cce547767d19f673e9d5b4450a35cba43f70e69b10b8ec86
Proof of Work: 847614847121939805773813989208
The Public key (e,n):
e: 17308001760157011025510890201746638424694908043834684046496043855417581675572879868824214949074886303482190253628656
```

(a) Damaged Manager

```
Digital Signature: 00A60428F2AFDF1810DF8CC50C9FA8B2854A63156978325C0F99E095539BA8A32BCBC0958585E92AEB478E4BFA0D1F46B85F
<<<<< End Blockchain >>>>>>>
【Consulte The Blockchain】
Contradiction
【This Blockchain does not match my Blockchain】
Provious Hash: 04b863729135e148ad1b1c18b078355386dafa0c8a7eaa6c09dc1d43be4e1814ac8cce547767d19f673e9d5b4450a35cba43f70e69b1
New DATA: 04FFDAA20DC637215684A886162F293E95CE9D462CD7A72F45FDDDB1279EAE66331623F7E15F590C3878151E668424CA31237CCE
Hash:  02700f4cd5a14d2dcbde5226a922e0bc44ef91afbaa70e21c6efe0cc1e422adc06bfc567343d2ae5e02e54f25b1c410d873e7164705219417211c
The Public key (e,n):
e: 17308001760157011025510890201746638424694908043834684046496043855417581675572879868824214949074886303482190253628656
n: 79052239432582855194046465675832674602486152968380663199969485651856992806863506298431527367625840331012477966124280
Digital Signature: 38492DDC21FC071E10D03B1562416F9E8A6CF165288979F9CED54BC9EF458BFF099E9F4FA7A3FA62F0872195E77E3D548713
<<<<< Start Blockchain >>>>>>>
-------- BLOCK N= 1--------
Provious Hash: 0000
New DATA: 00B6AFF133546E782F367348C225F008421A756AC00313DA13CAA741CFC32723FC6CC83A3D49EEAD02997AEC363DA4F72C573F82
Hash:  04b863729135e148ad1b1c18b078355386dafa0c8a7eaa6c09dc1d43be4e1814ac8cce547767d19f673e9d5b4450a35cba43f70e69b10b8ec86
Proof of Work: 847614847121939805773813989208
The Public key (e,n):
e: 17308001760157011025510890201746638424694908043834684046496043855417581675572879868824214949074886303482190253628656
```

(b) Received Manager

FIGURE 5.16: Integrity Attack.

5.5.1.3 Sniffing Attack

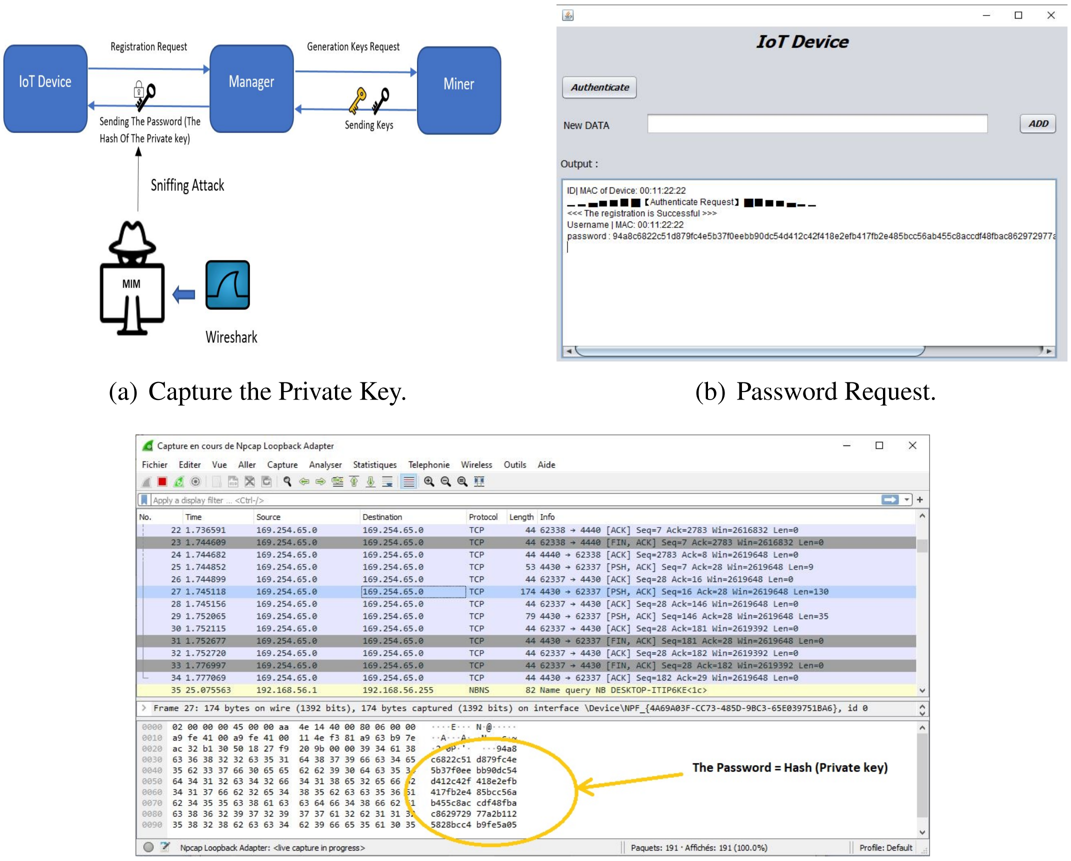
The information recorded in the blockchain may need managers and miners with high capacities, some companies which have effective resources (e.g. cloud computing) can adopt this service for the benefit of users, in this case, there will be a large distance between the managers and the IoT devices, causing malicious people that monitor the transmission between the two parties. These attackers are known as Man In the Middle (MIM), and this type of attack is known as Sniffing Attack. This threat exposes the network to two dangers:

- **Theft the Private Key:** If the IoT device which decrypts the encoded message, MIM steals the private key when the manager send it.
- **Monitoring the Clear Messages:** In the case where the manager is the decoder and the encoder, the MIM will monitor the clear information sent between them. On the other hand, if the manager is the decoder and the IoT device is the encoder, the MIM will only capture the clear messages sent from the manager to the IoT device.

Although the first attack is less frequent, it is much more dangerous than the second attack, because getting the private key allows the MIM to view all the victim confidential information recorded in the blockchain. To avoid these two types of threats, we have chosen the manager as decoded and encoder machine, in addition, we propose that the communication between the components should base on a protected channel by using the secure protocols (Table: 5.4). We applied a $SniffingAttack$ (Figure 5.17(a)) in order to capture the private key sent from the manager to the IoT device through the Wireshark tool [2]. We chose a capturing consists on the Npcap library [3] that can sniff the loopback packets. After the password request from the IoT device 5.17(b), our sniffing attack was successful and the Wireshark could capture the password 5.17(c). We note that obtaining the password -which is the hash of private key- does not enable a MIM to decrypt the messages. In addition, he cannot imitate the IoT device authentication due to the password is associated with the MAC address (Unique ID).

[2] https://www.wireshark.org/

[3] https://nmap.org/npcap/


IoT Device
Registration Request
Manager
Generation Keys Request
Miner
Sending The Password (The Hash Of The Private key)
Sending Keys
Sniffing Attack
MIM
Wireshark

(a) Capture the Private Key.

IoT Device

Authenticate
New DATA
ADD

Output :

```
ID| MAC of Device: 00:11:22:22
‗‗▄▄■■█【Authenticate Request】█■■▄‗‗
<<< The registration is Successful >>>
Username | MAC: 00:11:22:22
password : 94a8c6822c51d879fc4e5b37f0eebb90dc54d412c42f418e2efb417fb2e485bcc56ab455c8accdf48fbac862972977a
```

(b) Password Request.

Capture en cours de Npcap Loopback Adapter

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
Apply a display filter ... <Ctrl-/>

```
No.   Time         Source          Destination     Protocol Length Info
   22 1.736591     169.254.65.0    169.254.65.0    TCP       44 62338 → 4440 [ACK] Seq=7 Ack=2783 Win=2616832 Len=0
   23 1.744609     169.254.65.0    169.254.65.0    TCP       44 62338 → 4440 [FIN, ACK] Seq=7 Ack=2783 Win=2616832 Len=0
   24 1.744682     169.254.65.0    169.254.65.0    TCP       44 4440 → 62338 [ACK] Seq=2783 Ack=8 Win=2619648 Len=0
   25 1.744852     169.254.65.0    169.254.65.0    TCP       53 4430 → 62337 [PSH, ACK] Seq=7 Ack=28 Win=2619648 Len=9
   26 1.744899     169.254.65.0    169.254.65.0    TCP       44 62337 → 4430 [ACK] Seq=28 Ack=16 Win=2619648 Len=0
   27 1.745118     169.254.65.0    169.254.65.0    TCP      174 4430 → 62337 [PSH, ACK] Seq=16 Ack=28 Win=2619648 Len=130
   28 1.745156     169.254.65.0    169.254.65.0    TCP       44 62337 → 4430 [ACK] Seq=28 Ack=146 Win=2619648 Len=0
   29 1.752065     169.254.65.0    169.254.65.0    TCP       79 4430 → 62337 [PSH, ACK] Seq=146 Ack=28 Win=2619648 Len=35
   30 1.752115     169.254.65.0    169.254.65.0    TCP       44 62337 → 4430 [ACK] Seq=28 Ack=181 Win=2619392 Len=0
   31 1.752677     169.254.65.0    169.254.65.0    TCP       44 4430 → 62337 [FIN, ACK] Seq=181 Ack=28 Win=2619648 Len=0
   32 1.752720     169.254.65.0    169.254.65.0    TCP       44 62337 → 4430 [ACK] Seq=28 Ack=182 Win=2619392 Len=0
   33 1.776997     169.254.65.0    169.254.65.0    TCP       44 62337 → 4430 [FIN, ACK] Seq=28 Ack=182 Win=2619392 Len=0
   34 1.777069     169.254.65.0    169.254.65.0    TCP       44 4430 → 62337 [ACK] Seq=182 Ack=29 Win=2619648 Len=0
   35 25.075563    192.168.56.1    192.168.56.255  NBNS      82 Name query NB DESKTOP-ITIP6KE<1c>

> Frame 27: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface \Device\NPF_{4A69A03F-CC73-485D-9BC3-65E039751BA6}, id 0

0000  02 00 00 00 45 00 00 aa  4e 14 40 00 80 06 00 00   ····E··· N·@·····
0010  a9 fe 41 00 a9 fe 41 00  11 4e f3 81 a9 63 b9 7e   ··A···A· ·N···c·~
0020  ac 32 b1 30 50 18 27 f9  20 9b 00 00 39 34 61 38   ·2·0P·'· ····94a8
0030  63 36 38 32 32 63 35 31  64 38 37 39 66 63 34 65   c6822c51 d879fc4e
0040  35 62 33 37 66 30 65 65  62 62 39 30 64 63 35 34   5b37f0ee bb90dc54
0050  64 34 31 32 63 34 32 66  34 31 38 65 32 65 66 62   d412c42f 418e2efb
0060  34 31 37 66 62 32 65 34  38 35 62 63 63 35 36 61   417fb2e4 85bcc56a
0070  62 34 35 35 63 38 61 63  63 64 66 34 38 66 62 61   b455c8ac cdf48fba
0080  63 38 36 32 39 37 32 39  37 37 61 32 62 31 31 32   c8629729 77a2b112
0090  35 38 32 38 62 63 63 34  62 39 66 65 35 61 30 35   5828bcc4 b9fe5a05
```

The Password = Hash (Private key)

Npcap Loopback Adapter: <live capture in progress> | Paquets: 191 · Affichés: 191 (100.0%) | Profile: Default

(c) Wireshark Attack.

FIGURE 5.17: Sniffing Attack.

5.5.1.4 The dominance of Attackers

The dominance of the fraud (more than of 50% attackers) in the network makes the original blockchain lose its value. To prevent this type of threat, VCA (Algo: 6) was installed in the managers. It consists on the confidence criteria attributed, that is initialised by 1. To guarantee the legitimacy of the managers, through which, the managers will be divided into three ranks, Rank_A (their confidence criteria is high), Rank_B (their confidence criteria is average), and Rank_C (their confidence criteria is low). For each rank, VCA considers the following values: R_A= 80%, R_B= 60%, and R_C= 10%.

We fixed the number of legitimates managers to ten for all the tests as illustrated in Table 5.7. In the first phase, the network creates a blockchain of ten blocks and all blocks were accepted from 100% of managers. In the other tests, we increased the number of attackers which tampered our blockchain in order to convert it to a new one and make it the dominant. The results obtained are shown as a curve in Figure 5.18. We found that the higher is the threat, the acceptance rate of the new block is low.

Although the threat level was high in the the third, fourth, fifth and sixth tests (because the ratio of the threat is more or equal to 50%), the proposed VCA was able to accept the created block by a legitimate user. It is only rejected in the seventh test, and this does not mean that VCA has failed in this last test. In this case, a new configuration is created with the values (R_A=80%, R_B=60% and R_C=5%), and consequently the new block was accepted with 71%. Thus, most of attackers are in the rank C, which means, we should emphasize this rank, and focus on a safer rank such as rank A.

Test	T1	T2	T3	T4	T5	T6	T7
Number of legitimates	10	10	10	10	10	10	10
Number of All managers	10	15	20	25	40	50	60
percentage of Attackers	0%	30%	50%	60%	75%	40%	83.3%
percentage of Acceptation	100%	100%	83%	83%	62%	55%	50%

TABLE 5.7: The ratios of the acceptation of each test.

5.5.2 Access Control Issue

5.5.2.1 Network Configuration

In this part, we will transfer $\mathbb{SOT}-\mathbb{S}$ to a concrete work in order to confirm its smoothness and security level. $\mathbb{SOT}-\mathbb{S}$ components were developed into JAVA APIs. Our final network (Figure 5.19) is composed of $Advisor$, $Miner$, 10 $Subjects$ and 20 $Objects$. The advisor runs first, all machines contact it, and it receives the new subjects and objects requests and records their addresses. In the new subject and object contact, it provides them $RSA-Keys$ of 2048 bits (High secure) that are generated through the miner machine. Then, the new subjects will receive all blockchains network. The advisor is the unique machine that creates the new blocks (Figure 5.20). Then, it shares them with the subjects network, as for the smart contracts, they are implemented previously in the subject (is not taken from the blockchain), where, the rules shown in the figure

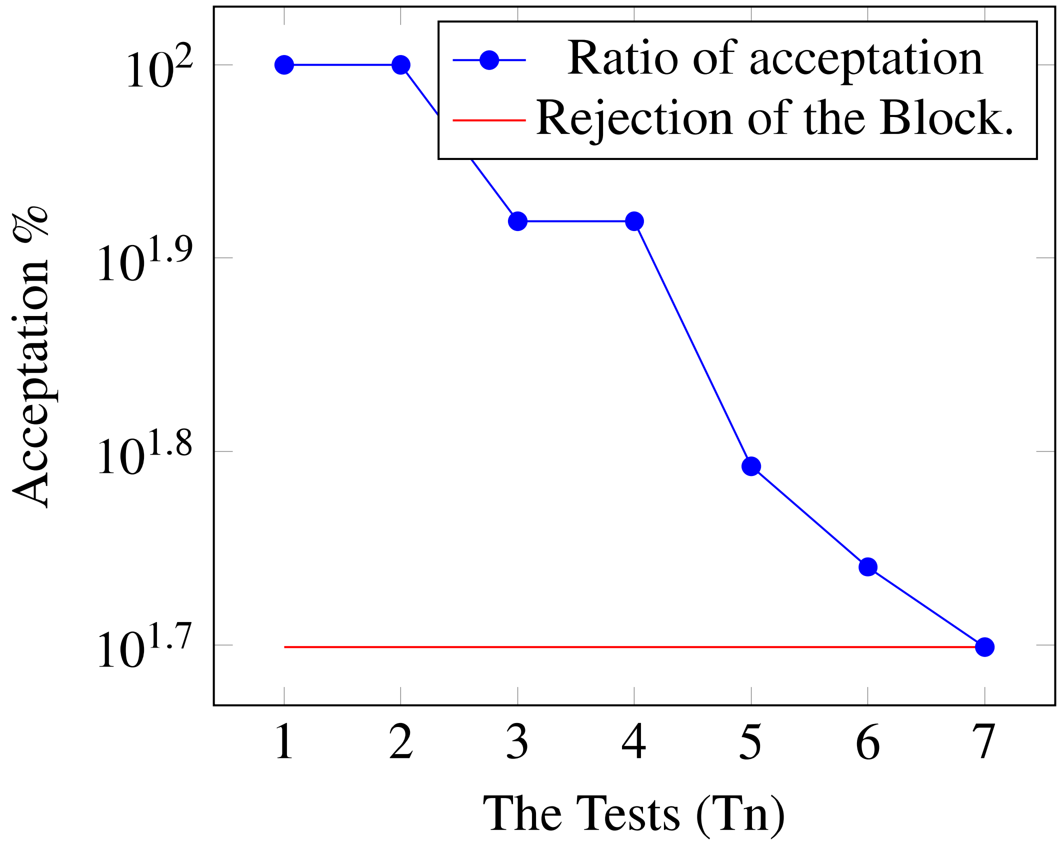


FIGURE 5.18: Ratios of acceptation of the new block for each test.

are for a description only. The miner is set to the hashing condition, which imposes every hash generated to start with at least one zero.

As we detailed previously (Figure 5.13), one subject can access to many objects after obtaining permission from the majority subjects (more than 50%). The latter checks the hash of the subject blockchains and the results of the smart contracts. Otherwise, the subject applicant receives a ban message, that explains the most likely reason for denying this access.

The first step of the tests is shown in Table 5.8. These access cases summarize all possibilities for which access can be accepted or denied. The test showed a smooth application without any conflict with our proposal and achieves the protection granted by the blockchain.

5.5.2.2 Control the level of protection

This stage confirms the proof of work, since the more difficult the hash condition, the fewer attackers. The hash is produced by combining block data with the proof of work. We conducted

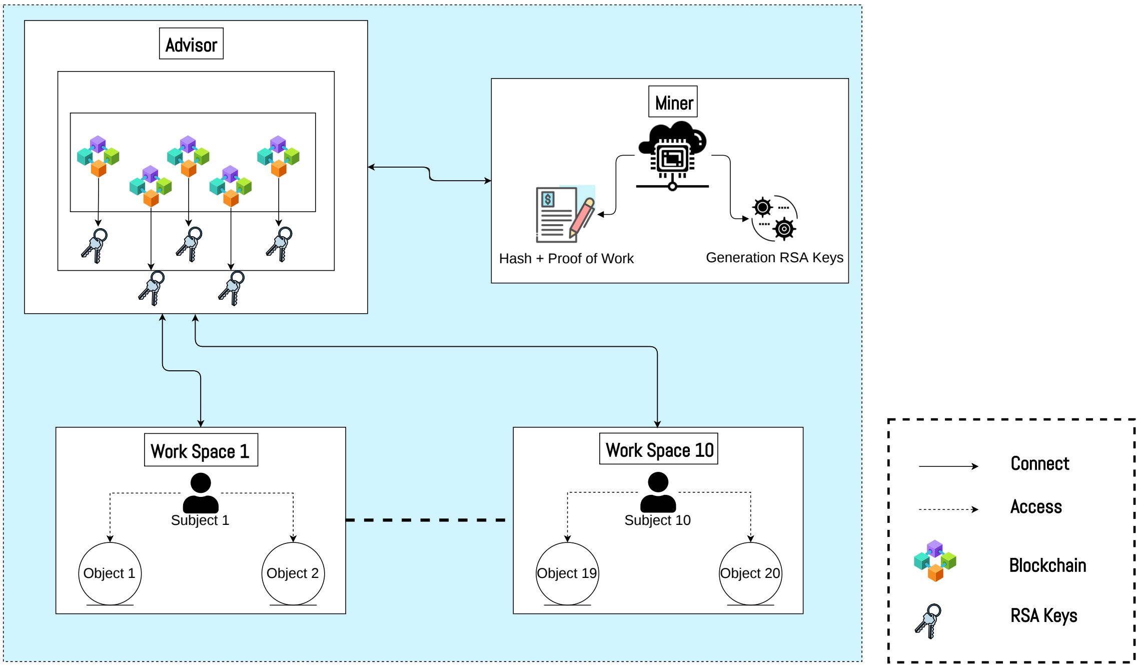
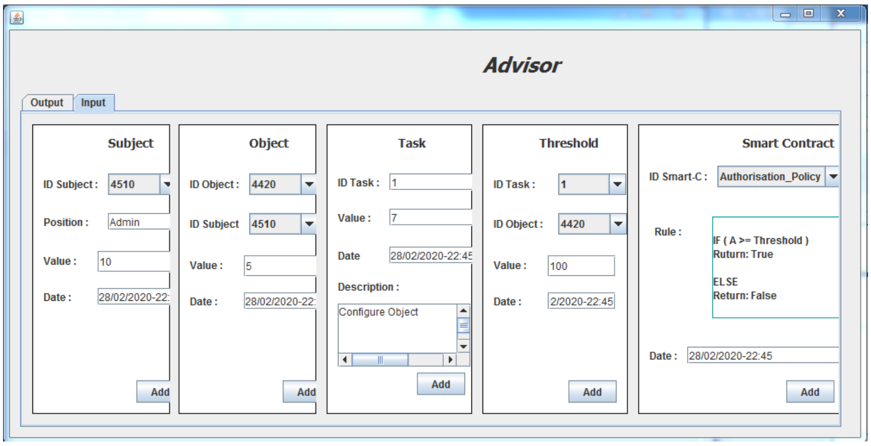


FIGURE 5.19: Access Control Network.



Advisor

Output | Input

Subject
ID Subject : 4510
Position : Admin
Value : 10
Date : 28/02/2020-22:

Object
ID Object : 4420
ID Subject 4510
Value : 5
Date : 28/02/2020-22:

Task
ID Task : 1
Value : 7
Date 28/02/2020-22:45
Description :
Configure Object

Threshold
ID Task : 1
ID Object : 4420
Value : 100
Date : 2/2020-22:45

Smart Contract
ID Smart-C : Authorisation_Policy
Rule :
IF (A >= Threshold)
Ruturn: True

ELSE
Return: False

Date : 28/02/2020-22:45

FIGURE 5.20: Advisor Dashboard.

increasingly difficult experiments. At the beginning, we did not restrict the miner to any condition. Then, in the second step, it had to produce a hash that starts with at least one zero. Thus, in the third step, it had to find a hash that starts with two zeros, and so on. In each experiment, we measured the time taken to produce a hash. The test results are shown in Figure 5.21. We conclude that the more difficult the condition, the greater is the duration of finding proof of work.

Some objects of high worth require tightening. This is done by raising its threshold with each task applied to it as shown by the experiment summarized in Figure 5.22. The number of accesses was counted for processes with fixed tasks, random subjects and objects. From the

Subject	**Object**	**Task**	**Access Value**	**Threshold**	**Current Access Value**	**Authen-tication**	**Priority**	**Permis-sion / Deny**
$S_1 = 5$	$O(O_1, S_1) = 5$	$T_1 = 5$	125	$Th(O_1 + T_1) = 100$	Null	✓	✓	✓
$S_1 = 5$	$O(O_2, S_1) = 5$	$T_2 = 2$	50	$Th(O_2 + T_2) = 100$	Null	✗	✓	✗
$S_2 = 5$	$O(O_3, S_2) = 10$	$T_1 = 5$	250	$Th(O_3 + T_1) = 40$	Null	✓	✓	✓
$S_1 = 5$	$O(O_3, S_1) = 2$	$T_1 = 5$	50	$Th(O_3 + T_1) = 40$	250	✓	✗	✗
$S_2 = 5$	$O(O_4, S_2) = 2$	$T_2 = 2$	20	$Th(O_4 + T_2) = 30$	Null	✗	✓	✗
$S_3 = 2$	$O(O_3, S_3) = 2$	$T_1 = 5$	20	$Th(O_3 + T_1) = 40$	250	✗	✗	✗

TABLE 5.8: Permission or Deny Access Controls.

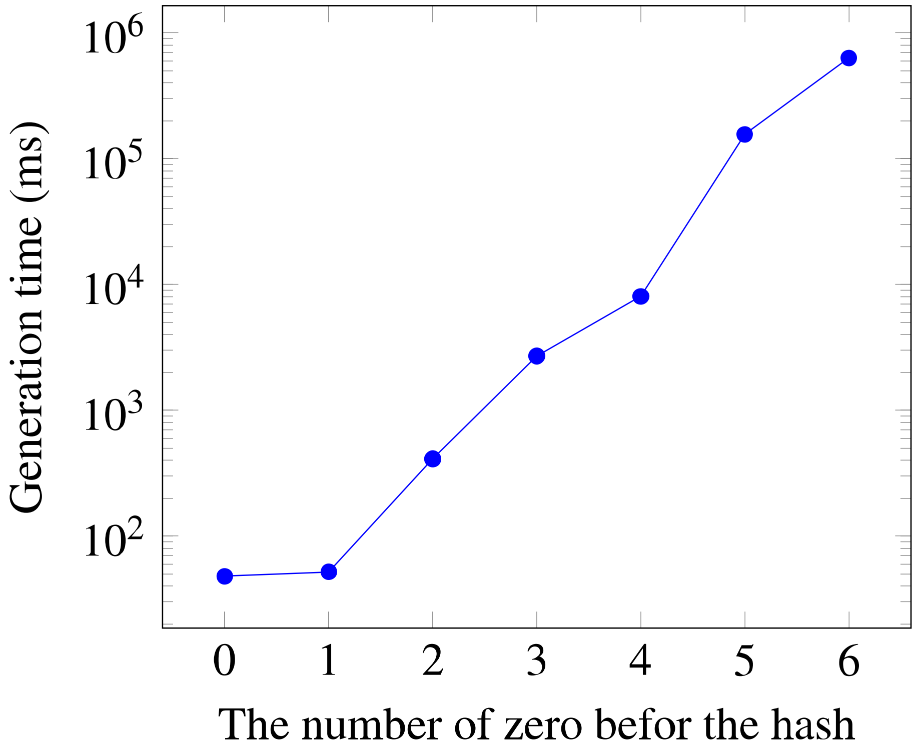


FIGURE 5.21: The relationship between the time taken and the difficulty of the condition.

obtained results, we conclude that the higher the threshold values for a given task and object, the smaller is the number of access on it.

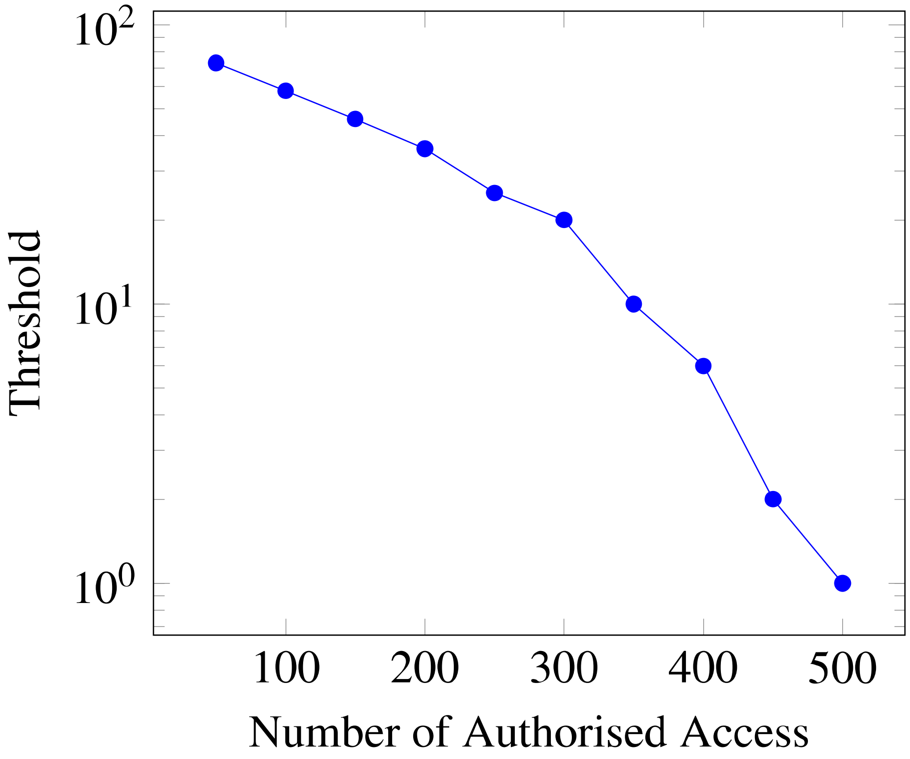


FIGURE 5.22: Increase the Difficulty Access through the Threshold.

5.6 Conclusion

In this chapter, we concentrated on the following issues. First, we developed a framework for protecting smart city information through blockchain technology. Secondly, we developed the framework, $\mathbb{SOT}-\mathbb{S}$, that controls access to objects by users (subjects) while taking into consideration permission and priority concepts. To protect $\mathbb{SOT}-\mathbb{S}$ parameters, we have included them within the blockchain. The conclusion of this thesis is presented in the next chapter. It summarizes the obtained results, and itemizes the next directions that extend the realized contributions.

Chapter 6

General Conclusion

The city is a large geographical area with a medium or high population density. Also, it is a symbol of civilization by its adoption of many public facilities in various fields such as health, transportation, education, finance, industry, etc. These aspects make it attractive to citizens who are looking for comfort, work, and safety life. This attraction results in challenges that could disrupt the healthy pace of the city such as increasing population density, high cost, sectors management, standardization of systems, protection of transmitted and stored information, environmental pollution, etc. Consequently, it required governments and researchers in this field to find solutions to keep pace with this remarkable change and to advance to a better state than before. The ideal solution is to make the city smart, by integrating modern technologies such as the IoT, AI, CPS, ICT, etc. This idea has grown among researchers, especially in the past years, as they have begun to propose contributions whose results are methodologies, architecture, frameworks, and other encouraging solutions in various fields (smart buildings, smart transportation, smart health, smart economy, smart government, etc.). Such solutions should have criteria that help continuity like data protection, low cost, permanent connection, unified network, speed of implementation, high quality, in addition, innovative contributions should be scalable, reliable, and smooth. The security issue in the smart city is an essential aspect due to the quality of city services depends on the correctness of the information. Blockchain is a modern technology that has seen great success after its use on electronic currencies, because it is based on transparency, where all network users participate in transactions, instead of having a third party manage the operations.

This thesis addressed the issue of protecting smart city information through blockchain technology. We have divided the work into three main stages, which are modeling, optimization, and security. In the modeling stage, we created architectures for buildings, and the city where we mentioned the digital components (such as protocols, encryption techniques, access control, etc.) and the physical components (sensors, servers, cloud computing, etc.) distributed over rooms, homes, buildings, and smart cities, where the supplies are derived from IoT technologies. In the optimization phase, we sought to reduce the cost and expand the coverage for WSNs (temperature sensors) taking into account the connectivity constraint. This is done by a developing a tool called, ISOD-NSGA 2. The latter used the multi-objective optimization algorithm NSGA 2 in addition to the innovative optimization algorithm (OSP). First, the area of the building is scanned,and take it as input, then the deploy-able solutions are extracted. The impacts of the obstacles are taken into account to detect the sensing and communication possibility. At the last stage, we considered two important aspects in the security field, which are protecting the integrity of information, and controlling access to devices using blockchain technology. For both sides, we proposed two approaches that incorporate nodes, communication protocols, and algorithms. We also referred to the SOT-S (Access Control System), which controls access to devices based on parameters (subject, object, task). It is based on an arithmetic reliable equation that gives a value indicating the right or denial of access.

In the future, we attend to expand our contributions by addressing other issues, especially:

- We aspire to take into account more security issues like confidentiality in the network, authenticity, etc, that can be harmed through divers attacks such as hollow flood, Exhaustion, Wormhole, etc.

- The BC size will be increased through time, so, the constrained devices will have difficulties adopting it in their limited memory. So, we can address this issue by developing their characteristics such as using nano memory, or proposing methods that reduce the BC size.

- Improving the latency network is an important issue, so we have to develop methods to solve it by considering the network parameters (distances, bandwidth, etc) and the geographical positions.

- Improving the optimal deployment of objects in large buildings while respecting the K-connectivity constraint and the impact of obstacles on the sensing and the communication operations. It is interesting also to compare our obtained results with updated ones.

- Our optimization contribution treats limited issues, therefore, we are interested in discussing other important issues like the heterogeneous sensors, moving, and environment phenomena (like reflection, refraction, and diffraction).
- The objects of other smart city domains (healthcare, transportation, etc) are characterized by different behaviors. So, we can study their interaction with each other through formal methods and networking techniques.
- In the security part, we intend to extend the developed framework to cover other protection mechanism like authentication and ensure the availability of the service. Also, our aim is to apply $\mathbb{SOT}-\mathbb{S}$ on real devices and use cases. In addition, we seek to compare our $\mathbb{SOT}-\mathbb{S}$ with other access control systems by taking into consideration the degree of protection, smoothness, scalability, etc.

Bibliography

[1] *Towards smart cities*. Apr. 2019. URL: https://en.unesco.org/courier/2019-2/towards-smart-cities.

[2] *Sustainable smart cities*. URL: https://unece.org/housing/sustainable-smart-cities.

[3] Leonidas Anthopoulos, Marijn Janssen, and Vishanth Weerakkody. "A Unified Smart City Model (USCM) for smart city conceptualization and benchmarking". In: *Smart cities and smart spaces: Concepts, methodologies, tools, and applications* (2019), pp. 247–264.

[4] Nicos Komninos et al. "Smart city ontologies: Improving the effectiveness of smart city applications". In: *Journal of Smart Cities (Transferred)* 1.1 (2016).

[5] Sally P Caird and Stephen H Hallett. "Towards evaluation design for smart city development". In: *Journal of urban Design* 24.2 (2019), pp. 188–209.

[6] Bo Tang et al. "A hierarchical distributed fog computing architecture for big data analysis in smart cities". In: *Proceedings of the ASE BigData & SocialInformatics 2015*. 2015, pp. 1–6.

[7] Nebojša Gavrilović and Alok Mishra. "Software architecture of the internet of things (IoT) for smart city, healthcare and agriculture: analysis and improvement directions". In: *Journal of Ambient Intelligence and Humanized Computing* 12.1 (2021), pp. 1315–1336.

[8] Nabaa Ali Jasim, Haider TH, and Salim AL Rikabi. "Design and Implementation of Smart City Applications Based on the Internet of Things." In: *International Journal of Interactive Mobile Technologies* 15.13 (2021).

[9] Harshith Arun Kumar et al. “Comparison of IoT architectures using a smart city benchmark”. In: *Procedia Computer Science* 171 (2020), pp. 1507–1516.

[10] Minglin Sun and Jian Zhang. “Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment”. In: *Computer Communications* 149 (2020), pp. 332–342.

[11] G Thippa Reddy et al. “Analysis of dimensionality reduction techniques on big data”. In: *IEEE Access* 8 (2020), pp. 54776–54788.

[12] Jinping Chang, Seifedine Nimer Kadry, and Sujatha Krishnamoorthy. “Review and synthesis of Big Data analytics and computing for smart sustainable cities”. In: *IET Intelligent Transport Systems* 14.11 (2020), pp. 1363–1370.

[13] Suriya Priya R Asaithambi, Ramanathan Venkatraman, and Sitalakshmi Venkatraman. “MOBDA: Microservice-Oriented Big Data Architecture for Smart City Transport Systems”. In: *Big Data and Cognitive Computing* 4.3 (2020), p. 17.

[14] Aapo Huovila et al. “Smart city performance measurement system”. In: *Proceedings of the 41th IAHS World Congress Sustainability Innovation for the Future, Algarve, Portugal*. 2016, pp. 13–16.

[15] Gartner*Inc. 3 trends surface in the Gartner Emerging Technologies Hype Cycle for 2021*. Aug. 2021. URL: https://www.gartner.com/smarterwithgartner/3-themes-surface-in-the-2021-hype-cycle-for-emerging-technologies.

[16] Eiman Al Nuaimi et al. “Applications of big data to smart cities”. In: *Journal of Internet Services and Applications* 6.1 (2015), pp. 1–15.

[17] Saraju P Mohanty, Uma Choppali, and Elias Kougianos. “Everything you wanted to know about smart cities: The internet of things is the backbone”. In: *IEEE Consumer Electronics Magazine* 5.3 (2016), pp. 60–70.

[18] Weihua Duan, Rouhollah Nasiri, and Sasan Karamizadeh. “Smart City Concepts and Dimensions”. In: *Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City*. 2019, pp. 488–492.

[19] Yasir Mehmood et al. "Internet-of-things-based smart cities: Recent advances and challenges". In: *IEEE Communications Magazine* 55.9 (2017), pp. 16–24.

[20] Mehmet Akif Destek and Avik Sinha. "Renewable, non-renewable energy consumption, economic growth, trade openness and ecological footprint: Evidence from organisation for economic Co-operation and development countries". In: *Journal of Cleaner Production* 242 (2020), p. 118537.

[21] Muhammad Khalid Anser. "Impact of energy consumption and human activities on carbon emissions in Pakistan: application of STIRPAT model". In: *Environmental Science and Pollution Research* 26.13 (2019), pp. 13453–13463.

[22] Emily Folk. - *the many economic benefits of renewable energy*. Mar. 2019. URL: https://www.renewableenergymagazine.com/emily-folk/the-many-economic-benefits-of-renewable-energy-20190312.

[23] Rajvikram Madurai Elavarasan et al. "A comprehensive review on renewable energy development, challenges, and policies of leading Indian states with an international perspective". In: *IEEE Access* 8 (2020), pp. 74432–74457.

[24] Arif Mahmud et al. "Simulation and comparison of RPL, 6Lowpan, and Coap protocols using Cooja simulator". In: *Proceedings of International Joint Conference on Computational Intelligence*. Springer. 2020, pp. 317–326.

[25] *Does an electric vehicle emit less than a petrol or diesel?* June 2022. URL: https://www.transportenvironment.org/discover/does-electric-vehicle-emit-less-petrol-or-diesel/.

[26] Sotnyk Iryna et al. "Green energy projects in households and its financial support in Ukraine". In: *International Journal of Sustainable Energy* 39.3 (2020), pp. 218–239. DOI: 10.1080/14786451.2019.1671389. eprint: https://doi.org/10.1080/14786451.2019.1671389. URL: https://doi.org/10.1080/14786451.2019.1671389.

[27] Henrik Lund et al. “Smart energy Denmark. A consistent and detailed strategy for a fully decarbonized society”. In: *Renewable and Sustainable Energy Reviews* 168 (2022), p. 112777.

[28] Shahzeb Haider et al. “A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks”. In: *Ieee Access* 8 (2020), pp. 53972–53983.

[29] *Five most famous ddos attacks and then some*. May 2022. URL: `https://www.a10networks.com/blog/5-most-famous-ddos-attacks/#:~:text=A%5C%20Brief%5C%20History%5C%20of%5C%20DDoS,become%5C%20a%5C%20classic%5C%20DDoS%5C%20attack..`

[30] Victor Garcia-Font, Carles Garrigues, and Helena Rifà-Pous. “Attack classification schema for smart city WSNs”. In: *Sensors* 17.4 (2017), p. 771.

[31] Mohammad Reza Mesbahi, Amir Masoud Rahmani, and Mehdi Hosseinzadeh. “Reliability and high availability in cloud computing environments: a reference roadmap”. In: *Human-centric Computing and Information Sciences* 8.1 (2018), pp. 1–31.

[32] Chai K Toh. “Security for smart cities”. In: *IET Smart Cities* 2.2 (2020), pp. 95–104.

[33] Shalli Rani and Sajjad Hussain Chauhdary. “A novel framework and enhanced QoS big data protocol for smart city applications”. In: *Sensors* 18.11 (2018), p. 3980.

[34] Francis Ogwu et al. “A Framework for Quality of Service in Mobile Ad Hoc”. In: *Int. Arab J. Inf. Technol.* 4 (Jan. 2007), pp. 33–40.

[35] Ammarah Cheema et al. “Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review”. In: *Security and Communication Networks* 2022 (May 2022), p. 8379532. ISSN: 1939-0114.

DOI: 10.1155/2022/8379532. URL: https://doi.org/10.1155/2022/8379532.

[36] Yang Yu et al. "Technology of short-distance wireless communication and its application based on equipment support". In: *AIP Conference Proceedings*. Vol. 1955. 1. AIP Publishing LLC. 2018, p. 040135.

[37] Krittin Intharawijitr, Katsuyoshi Iida, and Hiroyuki Koga. "Simulation study of low latency network architecture using mobile edge computing". In: *IEICE TRANSACTIONS on Information and Systems* 100.5 (2017), pp. 963–972.

[38] Sriganesh K Rao and Ramjee Prasad. "Impact of 5G technologies on smart city implementation". In: *Wireless Personal Communications* 100.1 (2018), pp. 161–176.

[39] URL: https://rantcell.com/comparison-of-2g-3g-4g-5g.html.

[40] Jiaoyan Chen and Jingsen Yang. "Maximizing coverage quality with budget constrained in mobile crowd-sensing network for environmental monitoring applications". In: *Sensors* 19.10 (2019), p. 2399.

[41] DS Vijayan et al. "Automation systems in smart buildings: a review". In: *Journal of Ambient Intelligence and Humanized Computing* (2020), pp. 1–13.

[42] Emmeline Woodward. *What are the types of smart building sensor and how do they work?* Nov. 2021. URL: https://www.pressac.com/insights/types-of-smart-building-sensor-and-how-they-work/.

[43] Cristian Perra et al. "Monitoring indoor people presence in buildings using low-cost infrared sensor array in doorways". In: *Sensors* 21.12 (2021), p. 4062.

[44] Kaspersky. *What is a ddos attack? - ddos meaning*. Feb. 2022. URL: https://www.kaspersky.com/resource-center/threats/ddos-attacks.

[45] Brian Dunbar. *What is a black hole?* May 2015. URL: https://www.nasa.gov/audience/forstudents/k-4/stories/nasa-knows/what-is-a-black-hole-k4.html.

[46] EC-Council. *What are sniffing attacks, and how can you protect yourself?nbsp;* June 2022. URL: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-are-sniffing-attacks/.

[47] Ghada Arfaoui et al. “A security architecture for 5G networks”. In: *IEEE Access* 6 (2018), pp. 22466–22479.

[48] Theodoros Zachariadis and Andreas Poullikkas. “The costs of power outages: A case study from Cyprus”. In: *Energy Policy* 51 (2012). Renewable Energy in China, pp. 630–641. ISSN: 0301-4215. DOI: https://doi.org/10.1016/j.enpol.2012.09.015. URL: https://www.sciencedirect.com/science/article/pii/S0301421512007732.

[49] Catia Cialani and Reza Mortazavi. “The cost of urban waste management: An empirical analysis of recycling patterns in Italy”. In: *Frontiers in Sustainable Cities* 2 (2020), p. 8.

[50] C.F. Calvillo, A. Sánchez-Miralles, and Jose Villar. “Energy management and planning in smart cities”. In: *Renewable and Sustainable Energy Reviews* 55 (Mar. 2016), pp. 273–287. DOI: 10.1016/j.rser.2015.10.133.

[51] Saurabh Shukla and Subrata Hait. “Smart waste management practices in smart cities: Current trends and future perspectives”. In: *Advanced Organic Waste Management*. Elsevier, 2022, pp. 407–424.

[52] Zaoui Sayah et al. “An intelligent system for energy management in smart cities based on big data and ontology”. In: *Smart and Sustainable Built Environment* (2020).

[53] Md Wahidur Rahman et al. “Intelligent waste management system using deep learning with IoT”. In: *Journal of King Saud University-Computer and Information Sciences* (2020).

[54] Dingfu Jiang. “The construction of smart city information system based on the Internet of Things and cloud computing”. In: *Computer Communications* 150 (2020), pp. 158–166.

[55] Jin Wang et al. “Big data service architecture: a survey”. In: *Journal of Internet Technology* 21.2 (2020), pp. 393–405.

[56] Julian Laufs, Hervé Borrion, and Ben Bradford. “Security and the smart city: A systematic review”. In: *Sustainable cities and society* 55 (2020), p. 102023.

[57] *Long-term trends in diabetes. April 2017*. eng. Report. Atlanta, GA, April 2017. URL: https://stacks.cdc.gov/view/cdc/46096.

[58] Bruna Alves. *U.S. retail electricity prices 2020*. July 2021. URL: https://www.statista.com/statistics/183700/us-average-retail-electricity-price-since-1990/.

[59] Martin Placek. *Car production: Number of cars produced worldwide 2018*. Aug. 2021. URL: https://www.statista.com/statistics/262747/worldwide-automobile-production-since-2000/.

[60] Published by Ian Tiseo and Nov 22. *Annual CO2 emissions worldwide from 1940 to 2020*. Nov. 2021. URL: https://www.statista.com/statistics/276629/global-co2-emissions/.

[61] *Global surface temperature*. Oct. 2021. URL: https://climate.nasa.gov/vital-signs/global-temperature/.

[62] *2021 Cyber Security Statistics Trends amp; Data*. Aug. 2021. URL: https://purplesec.us/resources/cyber-security-statistics/.

[63] Andres Monzon. “Smart cities concept and challenges: Bases for the assessment of smart city projects”. In: *2015 international conference on smart cities and green ICT systems (SMARTGREENS)*. IEEE. 2015, pp. 1–11.

[64] Hunt Allcott and Matthew Gentzkow. “Social media and fake news in the 2016 election”. In: *Journal of economic perspectives* 31.2 (2017), pp. 211–36.

[65] Stephan Lewandowsky et al. “Misinformation and its correction: Continued influence and successful debiasing”. In: *Psychological science in the public interest* 13.3 (2012), pp. 106–131.

[66] B Prabadevi and N Jeyanthi. “A review on various sniffing attacks and its mitigation techniques”. In: *Indones. J. Electr. Eng. Comput. Sci* 12.3 (2018), pp. 1117–1125.

[67] Nalini Subramanian and Andrews Jeyaraj. “Recent security challenges in cloud computing”. In: *Computers & Electrical Engineering* 71 (2018), pp. 28–42.

[68] Emmanouil Vasilomanolakis et al. “On the security and privacy of Internet of Things architectures and systems”. In: *2015 International Workshop on Secure Internet of Things (SIoT)*. IEEE. 2015, pp. 49–57.

[69] Walid Miloud Dahmane, Samir Ouchani, and Hafida Bouarfa. “Security Implementation and Verification in Smart Buildings”. In: *The 1st International Conference on Innovative Trends in Computer Science, CITSC 2019, Guelma, Algeria, November 20-21, 2019*. Ed. by Hamid Seridi et al. Vol. 2589. CEUR Workshop Proceedings. CEUR-WS.org, 2019, pp. 51–56. URL: `http://ceur-ws.org/Vol-2589/Paper8.pdf`.

[70] Walid Miloud Dahmane, Samir Ouchani, and Hafida Bouarfa. “A Smart Living Framework: Towards Analyzing Security in Smart Rooms”. In: *Model and Data Engineering - 9th International Conference, MEDI 2019, Toulouse, France, October 28-31, 2019, Proceedings*. Ed. by Klaus-Dieter Schewe and Neeraj Kumar Singh. Vol. 11815. Lecture Notes in Computer Science. Springer, 2019, pp. 206–215. DOI: `10.1007/978-3-030-32065-2\_15`. URL: `https://doi.org/10.1007/978-3-030-32065-2%5C_15`.

[71] Walid Miloud Dahmane, Samir Ouchani, and Hafida Bouarfa. “Towards a reliable smart city through formal verification and network analysis”. In: *Comput. Commun.* 180 (2021), pp. 171–187. DOI: `10.1016/j.comcom.2021.09.006`. URL: `https://doi.org/10.1016/j.comcom.2021.09.006`.

[72] Walid Miloud Dahmane et al. "A BIM-based framework for an Optimal WSN Deployment in Smart Building". In: *11th International Conference on Network of the Future, NoF 2020, Bordeaux, France, October 12-14, 2020*. Ed. by Prosper Chemouil et al. IEEE, 2020, pp. 110–114. DOI: 10.1109/NoF50125.2020.9249099. URL: https://doi.org/10.1109/NoF50125.2020.9249099.

[73] Walid Miloud Dahmane, Samir Ouchani, and Hafida Bouarfa. "Guaranteeing Information Integrity Through Blockchains for Smart Cities". In: *Model and Data Engineering - 10th International Conference, MEDI 2021, Tallinn, Estonia, June 21-23, 2021, Proceedings*. Ed. by J. Christian Attiogbé and Sadok Ben Yahia. Vol. 12732. Lecture Notes in Computer Science. Springer, 2021, pp. 199–212. DOI: 10.1007/978-3-030-78428-7_16. URL: https://doi.org/10.1007/978-3-030-78428-7%5C_16.

[74] Walid Miloud Dahmane, Samir Ouchani, and Hafida Bouarfa. "Guaranteeing information integrity and access control in smart cities through blockchain". In: *Journal of Ambient Intelligence and Humanized Computing* (2022), pp. 1–10.

[75] Raphael Cohen-Almagor. "Internet history". In: *Moral, ethical, and social dilemmas in the age of technology: Theories and practice*. IGI Global, 2013, pp. 19–39.

[76] Mohsen Attaran. "The impact of 5G on the evolution of intelligent automation and industry digitization". In: *Journal of Ambient Intelligence and Humanized Computing* (2021), pp. 1–17.

[77] Fatima Hameed Khan, Muhammad Adeel Pasha, and Shahid Masud. "Advancements in Microprocessor Architecture for Ubiquitous AI—An Overview on History, Evolution, and Upcoming Challenges in AI Implementation". In: *Micromachines* 12.6 (2021), p. 665.

[78] Dionisis Kandris et al. "Applications of wireless sensor networks: an up-to-date survey". In: *Applied System Innovation* 3.1 (2020), p. 14.

[79] Kirsi Laitala et al. "Increasing repair of household appliances, mobile phones and clothing: Experiences from consumers and the repair industry". In: *Journal of Cleaner Production* 282 (2021), p. 125349.

[80] Asif Nawaz et al. "Mode Inference using enhanced Segmentation and Pre-processing on raw Global Positioning System data". In: *Measurement and Control* 53.7-8 (2020), pp. 1144–1158.

[81] Quang-Huy Nguyen and Falko Dressler. "A smartphone perspective on computation offloading—a survey". In: *Computer Communications* 159 (2020), pp. 133–154.

[82] Sebastian Sadowski and Petros Spachos. "Wireless technologies for smart agricultural monitoring using internet of things devices with energy harvesting capabilities". In: *Computers and Electronics in Agriculture* 172 (2020), p. 105338.

[83] Petros Spachos. "Towards a low-cost precision viticulture system using internet of things devices". In: *IoT* 1.1 (2020), pp. 5–20.

[84] Marcela MATIUZZO. "Business models and big data: how google uses your personal information". In: *BRANCO, Sérgio; TEFFÉ, Chiara. Privacidade em perspectivas. Rio de Janeiro* (2018).

[85] Tanweer Alam. "A reliable communication framework and its use in internet of things (IoT)". In: *CSEIT1835111| Received* 10 (2018), pp. 450–456.

[86] Richard Chirgwin. *NTT demos petabit transmission on single fibre*. https://www.theregister.com/2012/09/23/ntt_petabit_fibre/. Last accessed 29 October 2021. 2012.

[87] *Cardiovascular diseases (CVDs)*. https://www.who.int/news-room/fact-sheets/detail/cardiovascular-diseases-(cvds). Last accessed 31 October 2021. 2021.

[88] *U.S. Fire Statistics*. https://www.usfa.fema.gov/data/statistics/. Last accessed 31 October 2021.

[89] *Tsunamis*. https://www.who.int/health-topics/tsunamis#tab=tab_1. Last accessed 31 October 2021.

[90] *WHO Coronavirus (COVID-19) Dashboard*. https://covid19.who.int/. Last accessed 31 October 2021.

[91] P Sihombing et al. "Development of building security integration system using sensors, microcontroller and GPS (Global Positioning System) based android smartphone". In: 978 (Mar. 2018), p. 012105. DOI: 10.1088/1742-6596/978/1/012105. URL: https://doi.org/10.1088/1742-6596/978/1/012105.

[92] Sarun Duangsuwan, Aekarong Takarn, and Punyawi Jamjareegulgarn. "A Development on Air Pollution Detection Sensors based on NB-IoT Network for Smart Cities". In: *2018 18th International Symposium on Communications and Information Technologies (ISCIT)*. 2018, pp. 313–317. DOI: 10.1109/ISCIT.2018.8587978.

[93] Ferdin Joe John Joseph. "IoT based weather monitoring system for effective analytics". In: *International Journal of Engineering and Advanced Technology* 8.4 (2019), pp. 311–315.

[94] Krishna Kumar, Narendra Kumar, and Rachna Shah. "Role of IoT to avoid spreading of COVID-19". In: *International Journal of Intelligent Networks* 1 (2020), pp. 32–35. ISSN: 2666-6030. DOI: https://doi.org/10.1016/j.ijin.2020.05.002. URL: https://www.sciencedirect.com/science/article/pii/S2666603020300026.

[95] Jenna Ross. *The Biggest Companies in the World in 2021*. https://www.visualcapitalist.com/the-biggest-companies-in-the-world-in-2021/. Last accessed 3 October 2021. 2021.

[96] PanJun Sun. "Security and privacy protection in cloud computing: Discussions and challenges". In: *Journal of Network and Computer Applications* 160 (2020), p. 102642.

[97] Abdellah Daissaoui et al. “IoT and big data analytics for smart buildings: a survey”. In: *Procedia Computer Science* 170 (2020), pp. 161–168.

[98] Yiqiao Chen and Elisabete A. Silva. “Smart transport: A comparative analysis using the most used indicators in the literature juxtaposed with interventions in English metropolitan areas”. In: *Transportation Research Interdisciplinary Perspectives* 10 (2021), p. 100371. ISSN: 2590-1982. DOI: https://doi.org/10.1016/j.trip.2021.100371. URL: https://www.sciencedirect.com/science/article/pii/S2590198221000786.

[99] Yi-Ching Lee, Lindsey A Malcein, and Sojung Claire Kim. “Information and communications technology (ICT) usage during COVID-19: Motivating factors and implications”. In: *International journal of environmental research and public health* 18.7 (2021), p. 3571.

[100] Kashif Hameed et al. “An intelligent IoT based healthcare system using fuzzy neural networks”. In: *Scientific Programming* 2020 (2020).

[101] Shaonan Shan et al. “Research on Collaborative Governance of Smart Government Based on Blockchain Technology: An Evolutionary Approach”. In: *Discrete Dynamics in Nature and Society* 2021 (2021).

[102] Jianguo Chen et al. “A survey on applications of artificial intelligence in fighting against COVID-19”. In: *ACM Computing Surveys (CSUR)* 54.8 (2021), pp. 1–32.

[103] Omar Abdel Wahab et al. “Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems”. In: *IEEE Communications Surveys & Tutorials* 23.2 (2021), pp. 1342–1397.

[104] Samira Pouyanfar et al. “A survey on deep learning: Algorithms, techniques, and applications”. In: *ACM Computing Surveys (CSUR)* 51.5 (2018), pp. 1–36.

[105] Zhongcheng Liu et al. “CPS-Based Human-Vehicle Co-Pilot Switching Strategy Under Different Information Flow Topologies”. In: *IEEE Access* 8 (2020), pp. 125943–125952.

[106] Fabian Müller, Christian Deuerlein, and Michael Koch. “Cyber-physical-system for representing a robot end effector”. In: *Procedia CIRP* 100 (2021), pp. 307–312.

[107] Smriti Bhatt and Ravi Sandhu. “Abac-cc: Attribute-based access control and communication control for internet of things”. In: *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*. 2020, pp. 203–212.

[108] Aechan Kim, Mohyun Park, and Dong Hoon Lee. “AI-IDS: Application of deep learning to real-time Web intrusion detection”. In: *IEEE Access* 8 (2020), pp. 70245–70261.

[109] Federico Seri et al. “Temperature Sensing Optimization for Home Thermostat Retrofit”. In: *Sensors* 21.11 (2021), p. 3685.

[110] Muhammad Umair et al. “Impact of COVID-19 on IoT Adoption in Healthcare, Smart Homes, Smart Buildings, Smart Cities, Transportation and Industrial IoT”. In: *Sensors* 21.11 (2021). ISSN: 1424-8220. DOI: 10.3390/s21113838. URL: https://www.mdpi.com/1424-8220/21/11/3838.

[111] Sunmi Jun et al. “Ultra-low-latency services in 5G systems: A perspective from 3GPP standards”. In: *ETRI Journal* 42.5 (2020), pp. 721–733.

[112] Zhen Li et al. “A Review of Smart Design Based on Interactive Experience in Building Systems”. In: *Sustainability* 12.17 (2020). ISSN: 2071-1050. DOI: 10.3390/su12176760. URL: https://www.mdpi.com/2071-1050/12/17/6760.

[113] Alaa Bani-Bakr et al. “Optimizing the number of fog nodes for finite fog radio access networks under multi-slope path loss model”. In: *Electronics* 9.12 (2020), p. 2175.

[114] Sangmin Lee et al. “Intelligent traffic control for autonomous vehicle systems based on machine learning”. In: *Expert Systems with Applications* 144 (2020), p. 113074.

[115] R Pradhap et al. “Solar Powered Hybrid Charging Station For Electrical Vehicle”. In: *International Journal of Engineering Technology Research & Management* 4.4 (2020), pp. 19–27.

[116] Abhishek Sharma et al. “Communication and networking technologies for UAVs: A survey”. In: *Journal of Network and Computer Applications* (2020), p. 102739.

[117] Giovanni Pau, Mario Collotta, and Vincenzo Maniscalco. “Bluetooth 5 Energy Management through a Fuzzy-PSO Solution for Mobile Devices of Internet of Things”. In: *Energies* 10 (July 2017). DOI: 10.3390/en10070992.

[118] Suk Hyun, Farhad Taghizadeh-Hesary, and Hyoung Suk Shim. “Modeling solar energy system demand using household-level data in Myanmar”. In: *Economic Analysis and Policy* 69 (2021), pp. 629–639.

[119] Ioannis Kougias. *Hydropower - Technology Development Report 2020*. Mar. 2021. DOI: 10.2760/825105.

[120] Kriti Yadav and Anirbid Sircar. “Geothermal energy provinces in India: A renewable heritage”. In: *International Journal of Geoheritage and Parks* 9.1 (2021), pp. 93–107.

[121] Ryan Wiser et al. “Expert elicitation survey predicts 37% to 49% declines in wind energy costs by 2050”. In: *Nature Energy* 6.5 (2021), pp. 555–565.

[122] Felix Günther. “Modeling advanced security aspects of key exchange and secure channel protocols”. In: *it-Information Technology* 62.5-6 (2020), pp. 287–293.

[123] Smriti Bhatt et al. “Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future”. In: *IEEE Access* 9 (2021), pp. 107200–107223.

[124] AWAN MAHMOOD. “Performance Analysis of Routing Protocols RIP, EIGRP, OSPF and IGRP using Networks connector”. In: (2020).

[125] N Saranya, K Geetha, and C Rajan. “Data replication in mobile edge computing systems to reduce latency in Internet of things”. In: *Wireless Personal Communications* 112.4 (2020), pp. 2643–2662.

[126] K Cornelius et al. “An efficient tracking system for air and sound pollution using IoT”. In: *2020 6th International conference on advanced computing and communication systems (ICACCS)*. IEEE. 2020, pp. 22–25.

[127] Ayca Kirimtat et al. “Future trends and current state of smart city concepts: A survey”. In: *IEEE Access* 8 (2020), pp. 86448–86467.

[128] Rondik J Hassan et al. “State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions”. In: *Asian Journal of Research in Computer Science* (2021), pp. 32–48.

[129] Elvira Ismagilova et al. “Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework”. In: *Information Systems Frontiers* (2020), pp. 1–22.

[130] Ghazaleh Javadzadeh and Amir Masoud Rahmani. “Fog computing applications in smart cities: A systematic survey”. In: *Wireless Networks* 26.2 (2020), pp. 1433–1457.

[131] Zainab Salih Ageed et al. “A survey of data mining implementation in smart city applications”. In: *Qubahan Academic Journal* 1.2 (2021), pp. 91–99.

[132] S Smys. “A Survey on Internet of Things (IoT) based Smart Systems”. In: *Journal of ISMAC* 2.04 (2020), pp. 181–189.

[133] Kuan Zhang et al. “Security and privacy in smart city applications: Challenges and solutions”. In: *IEEE Communications Magazine* 55.1 (2017), pp. 122–129.

[134] Loizos Kanaris et al. “On the realistic radio and network planning of IoT sensor networks”. In: *Sensors* 19.15 (2019), p. 3264.

[135] Marc Kacou et al. "A multi-wall and multi-frequency home environment path loss characterization and modeling". In: (2018).

[136] Mayank Raikwar et al. "A blockchain framework for insurance processes". In: *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE. 2018, pp. 1–4.

[137] Bin Liu et al. "Blockchain based data integrity service framework for IoT data". In: *2017 IEEE International Conference on Web Services (ICWS)*. IEEE. 2017, pp. 468–475.

[138] Ming Li et al. "Crowdbc: A blockchain-based decentralized framework for crowdsourcing". In: *IEEE Transactions on Parallel and Distributed Systems* 30.6 (2018), pp. 1251–1266.

[139] Deeraj Nagothu et al. "A microservice-enabled architecture for smart surveillance using blockchain technology". In: *2018 IEEE international smart cities conference (ISC2)*. IEEE. 2018, pp. 1–4.

[140] Sergii Kushch and Francisco Prieto-Castrillo. "Blockchain for dynamic nodes in a smart city". In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. IEEE. 2019, pp. 29–34.

[141] Bing Jia et al. "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks". In: *Sensors* 18.11 (2018), p. 3894.

[142] Mumin Cebe et al. "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles". In: *IEEE Communications Magazine* 56.10 (2018), pp. 50–57.

[143] Jordi Paillisse et al. "Distributed access control with blockchain". In: *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE. 2019, pp. 1–6.

[144] MD Azharul Islam and Sanjay Madria. “A permissioned blockchain based access control system for IOT”. In: *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE. 2019, pp. 469–476.

[145] Oscar Novo. “Blockchain meets IoT: An architecture for scalable access management in IoT”. In: *IEEE Internet of Things Journal* 5.2 (2018), pp. 1184–1195.

[146] Samir Ouchani. “Ensuring the Functional Correctness of IoT through Formal Modeling and Verification”. In: *Model and Data Engineering - 8th International Conference, MEDI 2018, Lecture Notes in Computer Science*. Springer International Publishing, 2018, pp. 401–417.

[147] Md Milon Islam, Ashikur Rahaman, and Md Rashedul Islam. “Development of smart healthcare monitoring system in IoT environment”. In: *SN computer science* 1 (2020), pp. 1–11.

[148] Tanweer Alam and Mohamed Benaida. “Blockchain and Internet of Things in Higher Education”. In: *Tanweer Alam, Mohamed Benaida." Blockchain and Internet of Things in Higher Education." Universal Journal of Educational Research* 8 (2020), pp. 2164–2174.

[149] Muhammad Baqer Mollah et al. “Blockchain for the internet of vehicles towards intelligent transportation systems: A survey”. In: *IEEE Internet of Things Journal* 8.6 (2020), pp. 4157–4185.

[150] Antonio M. Pascoal David Moreno-Salinas and Joaquin Aranda. “Optimal Sensor Placement for Multiple Target Positioning with Range-Only Measurements in Two-Dimensional Scenarios”. In: *Sensors* 13.8 (Aug. 2013). DOI: 10.3390/s130810674.

[151] A. Al-Fuqaha et al. “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”. In: *IEEE Communications Surveys Tutorials* 17.4 (Fourthquarter 2015), pp. 2347–2376. ISSN: 1553-877X. DOI: 10.1109/COMST.2015.2444095.

[152] A. Zanella et al. “Internet of Things for Smart Cities”. In: *IEEE Internet of Things Journal* 1.1 (Feb. 2014), pp. 22–32. ISSN: 2327-4662. DOI: 10.1109/JIOT.2014.2306328.

[153] Saraju P Mohanty, Uma Choppali, and Elias Kougianos. “Everything you wanted to know about smart cities: The internet of things is the backbone”. In: *IEEE Consumer Electronics Magazine* 5.3 (2016), pp. 60–70.

[154] M. Centenaro et al. “Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios”. In: *IEEE Wireless Communications* 23 (Oct. 2016).

[155] Luis Sanchez et al. “SmartSantander: IoT experimentation over a smart city testbed”. In: *Computer Networks* 61 (2014). Special issue on Future Internet Testbeds – Part I, pp. 217–238. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.bjp.2013.12.020. URL: http://www.sciencedirect.com/science/article/pii/S1389128613004337.

[156] Hemant Ghayvat et al. “WSN-and IOT-based smart homes and their extension to smart buildings”. In: *sensors* 15.5 (2015), pp. 10350–10379.

[157] S Arvind and V Anantha Narayanan. “An overview of security in CoAP: attack and analysis”. In: *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. IEEE. 2019, pp. 655–660.

[158] Dmitry G. Korzun, Sergey I. Balandin, and Andrei V. Gurtov. “Deployment of Smart Spaces in Internet of Things: Overview of the Design Challenges”. In: *Internet of Things, Smart Spaces, and Next Generation Networking*. Ed. by Sergey Balandin, Sergey Andreev, and Yevgeni Koucheryavy. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 48–59. ISBN: 978-3-642-40316-3.

[159] Giorgos Sfikas, Charilaos Akasiadis, and Evaggelos Spyrou. “Creating a Smart Room using an IoT approach”. In: May 2016.

[160] Arnold Janssens and Michel De Paepe. "Effect of moisture inertia models on the predicted indoor humidity in a room". In: *Proceedings of the 26th AIVC Conference* (Jan. 2005).

[161] Dhiren Tejani, Ali Al-Kuwari, and Vidyasagar Potdar. "Energy conservation in a smart home". In: (May 2011). DOI: 10.1109/DEST.2011.5936632.

[162] Konglong Tang et al. "Design and Implementation of Push Notification System Based on the MQTT Protocol". In: *2013 International Conference on Information Science and Computer Applications (ISCA 2013)*. Atlantis Press, 2013/10. ISBN: 978-90786-77-85-7. DOI: https://doi.org/10.2991/isca-13.2013.20. URL: https://doi.org/10.2991/isca-13.2013.20.

[163] *Uppaal Home*. http://www.uppaal.org/. 2019.

[164] Dr. Lakshmi Devasena C. "IPv6 low power wireless personal area network (6LoWPAN) for networking Internet of Things (IoT) - Analyzing its suitability for IoT". In: 9 (Jan. 2016). DOI: 10.17485/ijst/2016/v9i30/98730.

[165] S. Andreev et al. "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap". In: *IEEE Communications Magazine* 53.9 (Sept. 2015), pp. 32–40. ISSN: 0163-6804. DOI: 10.1109/MCOM.2015.7263370.

[166] Xenofon Fafoutis et al. "On Predicting the Battery Lifetime of IoT Devices: Experiences from the SPHERE Deployments". In: *Proceedings of the 7th International Workshop on Real-World Embedded Wireless Systems and Networks*. RealWSN'18. Shenzhen, China: ACM, 2018, pp. 7–12. ISBN: 978-1-4503-6048-7. DOI: 10.1145/3277883.3277892. URL: http://doi.acm.org/10.1145/3277883.3277892.

[167] Sachin Babar et al. "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)". In: *Recent Trends in Network Security and Applications*. Ed. by Natarajan Meghanathan et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 420–429. ISBN: 978-3-642-14478-3.

[168] A. Sehgal et al. "Management of resource constrained devices in the internet of things". In: *IEEE Communications Magazine* 50.12 (Dec. 2012), pp. 144–149. ISSN: 0163-6804. DOI: 10.1109/MCOM.2012.6384464.

[169] M. Aazam and E. Huh. "Fog Computing Micro Datacenter Based Dynamic Resource Estimation and Pricing Model for IoT". In: *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*. Mar. 2015, pp. 687–694. DOI: 10.1109/AINA.2015.254.

[170] P. Desai, A. Sheth, and P. Anantharam. "Semantic Gateway as a Service Architecture for IoT Interoperability". In: *2015 IEEE International Conference on Mobile Services*. June 2015, pp. 313–319. DOI: 10.1109/MobServ.2015.51.

[171] Amos Kingatua. *IoT System Tests :: Checking for Failure*. URL: https://medium.com/supplyframe-hardware/iot-system-tests-checking-for-failure-c146d2ebb8ef.

[172] Y. Chen and T. Kunz. "Performance evaluation of IoT protocols under a constrained wireless access network". In: *2016 International Conference on Selected Topics in Mobile Wireless Networking (MoWNeT)*. Apr. 2016, pp. 1–7. DOI: 10.1109/MoWNet.2016.7496622.

[173] G. Xiao et al. "User Interoperability With Heterogeneous IoT Devices Through Transformation". In: *IEEE Transactions on Industrial Informatics* 10.2 (May 2014), pp. 1486–1496. ISSN: 1551-3203. DOI: 10.1109/TII.2014.2306772.

[174] *IOT SENSORS*. https://fiware-tutorials.readthedocs.io/en/latest/iot-sensors/. 2019.

[175] Q. Zhu et al. "IOT Gateway: BridgingWireless Sensor Networks into Internet of Things". In: *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*. Dec. 2010, pp. 347–352. DOI: 10.1109/EUC.2010.58.

[176] Luigi Atzori, Antonio Iera, and Giacomo Morabito. “The Internet of Things: A Survey”. In: *Comput. Netw.* 54.15 (Oct. 2010), pp. 2787–2805. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2010.05.010. URL: http://dx.doi.org/10.1016/j.comnet.2010.05.010.

[177] *MQTT*. http://mqtt.org/. May 2019.

[178] Avijit Mallik et al. “Man-in-the-middle-attack: Understanding in simple words”. In: 3 (Jan. 2019), pp. 77–92. DOI: 10.5267/j.ijdns.2019.1.001.

[179] Rajeev Sobti and Geetha Ganesan. “Cryptographic Hash Functions: A Review”. In: *International Journal of Computer Science Issues, ISSN (Online): 1694-0814* Vol 9 (Mar. 2012), pp. 461–479.

[180] Jean-François Blanchette. “The digital signature dilemma Le dilemme de la signature numérique”. In: 2006.

[181] A. Wool. “A quantitative study of firewall configuration errors”. In: *Computer* 37.6 (June 2004), pp. 62–67. ISSN: 0018-9162. DOI: 10.1109/MC.2004.2.

[182] David Ferraiolo and D Kuhn. “Role-Based Access Controls”. In: (Mar. 2009).

[183] Shipra Suman and Aditi Agrawal. “IP Traffic Management With Access Control List Using Cisco Packet Tracer”. In: *International Journal of Science, Engineering and Technology Research* 5 (May 2016), pp. 1556–1561.

[184] Mick O Brien and George Weir. “Understanding digital certificates”. In: (June 2019).

[185] Edward A Lee. “Cyber physical systems: Design challenges”. In: *2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)*. IEEE. 2008, pp. 363–369.

[186] Renata Paola Dameri. “Searching for smart city definition: a comprehensive proposal”. In: *International Journal of computers & technology* 11.5 (2013), pp. 2544–2551.

[187] Jayavardhana Gubbi et al. “Internet of Things (IoT): A vision, architectural elements, and future directions”. In: *Future generation computer systems* 29.7 (2013), pp. 1645–1660.

[188] Keyur K Patel, Sunil M Patel, et al. “Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges”. In: *International journal of engineering science and computing* 6.5 (2016).

[189] Zhi-Kai Zhang et al. “IoT security: ongoing challenges and research opportunities”. In: *2014 IEEE 7th international conference on service-oriented computing and applications*. IEEE. 2014, pp. 230–234.

[190] Zaheer Allam and Peter Newman. “Redefining the smart city: Culture, metabolism and governance”. In: *Smart Cities* 1.1 (2018), pp. 4–25.

[191] Bharathan Balaji et al. “Brick: Metadata schema for portable smart building applications”. In: *Applied energy* 226 (2018), pp. 1273–1292.

[192] Petar Radanliev et al. “Definition of Internet of Things (IoT) Cyber Risk–Discussion on a Transformation Roadmap for Standardisation of Regulations, Risk Maturity, Strategy Design and Impact Assessment”. In: (2019).

[193] Gerd Behrmann, Alexandre David, and Kim G Larsen. “A tutorial on uppaal”. In: *Formal methods for the design of real-time systems* (2004), pp. 200–236.

[194] Mohamed Abdel-Basset, Mai Mohamed, and Victor Chang. “NMCDA: A framework for evaluating cloud computing services”. In: *Future Generation Computer Systems* 86 (2018), pp. 12–29.

[195] Jasenka Dizdarević et al. “A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration”. In: *ACM Computing Surveys (CSUR)* 51.6 (2019), pp. 1–29.

[196] Akbar Iskandar, Elisabet Virma, and Ansari Saleh Ahmar. “Implementing DMZ in improving network security of web testing in STMIK AKBA”. In: *arXiv preprint arXiv:1901.04081* (2019).

[197] Sinh-Ngoc Nguyen et al. “Design and implementation of intrusion detection system using convolutional neural network for DoS detection”. In: *Proceedings of the 2nd international conference on machine learning and soft computing*. 2018, pp. 34–38.

[198] Rishabh Das, Vineetha Menon, and Thomas H Morris. “On the edge realtime intrusion prevention system for dos attack”. In: *5th International Symposium for ICS & SCADA Cyber Security Research 2018 5*. 2018, pp. 84–91.

[199] Osamah Ibrahim Khalaf and Bayan Mahdi Sabbar. “An overview on wireless sensor networks and finding optimal location of nodes”. In: *Periodicals of Engineering and Natural Sciences (PEN)* 7.3 (2019), pp. 1096–1101.

[200] Monowar Hasan and Sibin Mohan. “Protecting actuators in safety-critical IoT systems from control spoofing attacks”. In: *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*. 2019, pp. 8–14.

[201] Won-il Bae and Jin Kwak. “Smart card-based secure authentication protocol in multi-server IoT environment”. In: *Multimedia Tools and Applications* 79.23 (2020), pp. 15793–15811.

[202] Salah A Alabady, Fadi Al-Turjman, and Sadia Din. “A novel security model for cooperative virtual networks in the IoT era”. In: *International Journal of Parallel Programming* 48.2 (2020), pp. 280–295.

[203] Ming Chang and Min Zhang. “Architecture Design of Datacenter for Cloud English Education Platform.” In: *International Journal of Emerging Technologies in Learning* 14.1 (2019).

[204] Angelo Capossele et al. “Security as a CoAP resource: an optimized DTLS implementation for the IoT”. In: *2015 IEEE international conference on communications (ICC)*. IEEE. 2015, pp. 549–554.

[205] Nitin Naik. “Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP”. In: *2017 IEEE international systems engineering symposium (ISSE)*. IEEE. 2017, pp. 1–7.

[206] Henghua Shi, Renlong Zhang, and Yujie Wang. “Learning and Teaching the Communication Between VLANs with Three Layer Switch”. In: *2015 International Conference on Management, Education, Information and Control*. Atlantis Press. 2015, pp. 1271–1275.

[207] Tariq Javid, Tehseen Riaz, and Asad Rasheed. “A layer2 firewall for software defined network”. In: *2014 Conference on Information Assurance and Cyber Security (CIACS)*. IEEE. 2014, pp. 39–42.

[208] Sohely Jahan, Md Saifur Rahman, and Sajeeb Saha. “Application specific tunneling protocol selection for Virtual Private Networks”. In: *2017 International Conference on Networking, Systems and Security (NSysS)*. IEEE. 2017, pp. 39–44.

[209] Ahmadreza Montazerolghaem et al. “A load scheduler for SIP proxy servers: design, implementation and evaluation of a history weighted window approach”. In: *International Journal of Communication Systems* 30.3 (2017), e2980.

[210] Zakariae Tbatou et al. “A New Mutuel Kerberos Authentication Protocol for Distributed Systems.” In: *Int. J. Netw. Secur.* 19.6 (2017), pp. 889–898.

[211] Byungho Min et al. “Antivirus security: naked during updates”. In: *Software: Practice and Experience* 44.10 (2014), pp. 1201–1222.

[212] Ilias Mavridis and Helen Karatza. “Performance evaluation of cloud-based log file analysis with Apache Hadoop and Apache Spark”. In: *Journal of Systems and Software* 125 (2017), pp. 133–151.

[213] Qian Zhongsheng, Li Xin, and Wang Xiaojin. “Modeling Distributed Real-time Elevator System by Three Model Checkers”. In: *International Journal of Online Engineering (iJOE)* 14 (Apr. 2018), p. 94. DOI: 10.3991/ijoe.v14i04.8383.

[214] Zamira Daw and Rance Cleaveland. “Comparing model checkers for timed UML activity diagrams”. In: *Science of Computer Programming* 111 (2015), pp. 277–299.

[215] Aaamir Naeem et al. “Comparison of Model Checking Tools Using Timed Automata - PRISM and UPPAAL”. In: *2018 IEEE International Conference on Computer and Communication Engineering Technology (CCET)*. 2018, pp. 248–253. DOI: 10.1109/CCET.2018.8542231.

[216] E. Bortnik et al. *Analyzing a Chi model of a turntable system using Spin, CADP and Uppaal*. English. Computer science reports. Technische Universiteit Eindhoven, 2004.

[217] Franco Mazzanti and Alessio Ferrari. “Ten diverse formal models for a CBTC automatic train supervision system”. In: *arXiv preprint arXiv:1803.10324* (2018).

[218] Kévin Roussel, Ye-Qiong Song, and Olivier Zendra. “Using Cooja for WSN simulations: some new uses and limits”. In: *EWSN 2016—NextMote workshop*. Junction Publishing. 2016, pp. 319–324.

[219] Leila Ben Saad, Cedric Chauvenet, and Bernard Tourancheau. “Simulation of the RPL Routing Protocol for IPv6 Sensor Networks: two cases studies”. In: *International Conference on Sensor Technologies and Applications SENSORCOMM 2011*. IARIA. 2011.

[220] Laurynas Riliskis and Evgeny Osipov. “Symphony: A Framework for Accurate and Holistic WSN Simulation”. In: *A C M Transactions on Embedded Computing Systems* 15 (Jan. 2013). DOI: 10.3390/s150304677.

[221] Mamoun Qasem et al. “Performance evaluation of RPL objective functions”. In: *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*. IEEE. 2015, pp. 1606–1613.

[222] *Electricity consumption comparisons for home appliances and electron-ics*. https://www.reliant.com/en/residential/electricity/save-energy/tips-to-lower-your-electricity-bill/electricity-consumption-comparison.jsp. Accessed: 2020.

[223] Zhanbo Xu et al. “Performance analysis and comparison on energy storage devices for smart building energy management”. In: *IEEE Transactions on Smart Grid* 3.4 (2012), pp. 2136–2147.

[224] Jianchao Zhang, Boon-Chong Seet, and Tek Tjing Lie. “Building information modelling for smart built environments”. In: *Buildings* 5.1 (2015), pp. 100–115.

[225] Kai-Ming Chang, Ren-Jye Dzeng, and Yi-Ju Wu. “An automated IoT visualization BIM platform for decision support in facilities management”. In: *Applied sciences* 8.7 (2018), p. 1086.

[226] Abdusy Syarif et al. “Performance analysis of evolutionary multi-objective based approach for deployment of wireless sensor network with the presence of fixed obstacles”. In: *2014 IEEE Global Communications Conference*. IEEE. 2014, pp. 1–6.

[227] Xuxun Liu. “A deployment strategy for multiple types of requirements in wireless sensor networks”. In: *IEEE Transactions on Cybernetics* 45.10 (2015), pp. 2364–2376.

[228] JSC Turner et al. “Modelling indoor propagation for WSN deployment in smart building”. In: *2014 2nd international conference on electronic design (ICED)*. IEEE. 2014, pp. 398–402.

[229] Reza Javanmard Alitappeh, Kossar Jeddisaravi, and Frederico G Guimarães. “Multi-objective multi-robot deployment in a dynamic environment”. In: *Soft Computing* 21.21 (2017), pp. 6481–6497.

[230] Abdelkader Raghib, Badr Abou El Majd, and Brahim Aghezzaf. “An optimal deployment of readers for rfid network planning using nsga-ii”. In: *Recent Developments in Metaheuristics*. Springer, 2018, pp. 463–476.

[231] Yourim Yoon and Yong-Hyuk Kim. “An efficient genetic algorithm for maximum coverage deployment in wireless sensor networks”. In: *IEEE Transactions on Cybernetics* 43.5 (2013), pp. 1473–1483.

[232] Mohamed Amin Benatia et al. “Multi-objective WSN deployment using genetic algorithms under cost, coverage, and connectivity constraints”. In: *Wireless Personal Communications* 94.4 (2017), pp. 2739–2768.

[233] Loizos Kanaris et al. “On the realistic radio and network planning of IoT sensor networks”. In: *Sensors* 19.15 (2019), p. 3264.

[234] Hemant Ghayvat et al. “WSN-and IOT-based smart homes and their extension to smart buildings”. In: *Sensors* 15.5 (2015), pp. 10350–10379.

[235] Pratit Nayak, Ekta Nashine, and Sanjeet Kumar. “Deployment of a Wireless Sensor Network in the Presence of Obstacle and Its Performance Evaluation”. In: *Advances in Signal Processing and Communication*. Springer, 2019, pp. 85–93.

[236] Yahia Tachwali, Hazem Refai, and John E Fagan. “Minimizing HVAC energy consumption using a wireless sensor network”. In: *IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society*. IEEE. 2007, pp. 439–444.

[237] Hongxia Wang et al. “Integration of BIM and live sensing information to monitor building energy performance”. In: *Proceedings of the 30th CIB W78 International Conference*. Vol. 30. 2013, pp. 344–352.

[238] Sameer Sundresh, Wooyoung Kim, and Gul Agha. “SENS: A sensor, environment and network simulator”. In: *37th Annual Simulation Symposium, 2004. Proceedings.* IEEE. 2004, pp. 221–228.

[239] Anit Kumar. “Encoding schemes in genetic algorithm”. In: *International Journal of Advanced Research in IT and Engineering* 2.3 (2013), pp. 1–7.

[240] David Lizcano et al. “Blockchain-based approach to create a model of trust in open and ubiquitous higher education”. In: *Journal of Computing in Higher Education* 32.1 (2020), pp. 109–134.

[241] Tanweer Alam and Mohamed Benaida. “Blockchain and Internet of Things in Higher Education”. In: *Tanweer Alam, Mohamed Benaida." Blockchain and Internet of Things in Higher Education." Universal Journal of Educational Research* 8 (2020), pp. 2164–2174.

[242] Han Sun, Xiaoyue Wang, and Xinge Wang. “Application of Blockchain Technology in Online Education.” In: *International Journal of Emerging Technologies in Learning* 13.10 (2018).

[243] Antonio Celesti et al. “Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds”. In: *Sensors* 20.9 (2020), p. 2590.

[244] Geetanjali Rathee et al. “A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology”. In: *Multimedia Tools and Applications* 79.15 (2020), pp. 9711–9733.

[245] Marijn Janssen et al. “A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors”. In: *International Journal of Information Management* 50 (2020), pp. 302–309.

[246] Ao Lei et al. “Blockchain-based dynamic key management for heterogeneous intelligent transportation systems”. In: *IEEE Internet of Things Journal* 4.6 (2017), pp. 1832–1843.

[247] Noe Elisa et al. “A framework of blockchain-based secure and privacy-preserving E-government system”. In: *Wireless Networks* (2018), pp. 1–11.

[248] Engineering National Academies of Sciences and Medicine. *Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions*. Ed. by Lynette I. Millett, Baruch Fischhoff, and Peter J. Weinberger. Washington, DC: The National Academies Press, 2017. ISBN: 978-0-309-45529-9. DOI: 10.17226/

24676. URL: https://www.nap.edu/catalog/24676/foundational-cybersecurity-research-improving-science-engineering-and-institutions.

[249] Michael Hochman Fuchs et al. *Why Americans Should Care about Russian Hacking*. Center for American Progress, 2017.

[250] Loic Lesavre et al. "A taxonomic approach to understanding emerging blockchain identity management systems". In: *arXiv preprint arXiv:1908.00929* (2019).

[251] Ali Maetouq et al. "Comparison of hash function algorithms against attacks: A review". In: *International Journal of Advanced Computer Science and Applications, br* 8 (2018).

[252] Yantao Li, Guangfu Ge, and Dawen Xia. "Chaotic hash function based on the dynamic S-Box with variable parameters". In: *Nonlinear Dynamics* 84.4 (2016), pp. 2387–2402.

[253] Yantao Li, Xiang Li, and Xiangwei Liu. "A fast and efficient hash function based on generalized chaotic mapping with variable parameters". In: *Neural Computing and Applications* 28.6 (2017), pp. 1405–1415.

[254] Michal Turčanık and Martin Javurek. "Hash function generation by neural network". In: *2016 New Trends in Signal Processing (NTSP)*. IEEE. 2016, pp. 1–5.

[255] Musheer Ahmad et al. "A simple secure hash function scheme using multiple chaotic maps". In: *3D Research* 8.2 (2017), p. 13.

[256] B Padmavathi and S Ranjitha Kumari. "A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution". In: *IJSR, India* 2 (2013), pp. 2319–7064.

[257] Avijit Mallik et al. "Man-in-the-middle-attack: Understanding in simple words". In: 3 (Jan. 2019), pp. 77–92. DOI: 10.5267/j.ijdns.2019.1.001.

[258] Mikail Mohammed Salim, Shailendra Rathore, and Jong Hyuk Park. “Distributed denial of service attacks and its defenses in IoT: a survey”. In: *The Journal of Supercomputing* 76.7 (2020), pp. 5320–5363.