PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
Ministry of Higher Education and Scientific Research
University of Mohamed Khider – Biskra

Faculty of Exact Sciences,
Sciences of Natural and Life

Computer Science
Department

Order number: ……

THESIS
Presented in order to obtain the degree of
DOCTOR 3rd CYCLE LMD IN COMPUTER SCIENCE
Option: Artificial Intelligence

Title

An Agent-Based Approach for the Internet of Things

Defended by
Maroua AHMID

Before the jury composed of:

Chairman	**Pr.** Mohamed Tayeb LASKRI	University of Annaba
Supervisor	**Pr.** Okba KAZAR	University of Biskra
Co- Supervisor	**Pr.** Laid KAHLOUL	University of Biskra
Examiner	**Pr.** Faiza KHELLAF	University of USTHB
Examiner	**Pr.** Khaled REZEG	University of Biskra
Invited	**Pr.** Malika IOUALALEN	University of USTHB

2021/2022

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider – BISKRA

Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie

Département d'informatique

N° d'ordre: ……

THÈSE
Présentée en vue de l'obtention du diplôme de
DOCTORAT 3ème CYCLE LMD EN INFORMATIQUE
Option: Intelligence Artificielle

Titre

Une Approche Basée Agent pour l'Internet des Objets

Présentée par
Maroua AHMID

Devant le jury composé de:

Président	**Pr.** Mohamed Tayeb LASKRI	Université d'Annaba
Rapporteur	**Pr.** Okba KAZAR	Université de Biskra
Co-Rapporteur	**Pr.** Laid KAHLOUL	Université de Biskra
Examinateur	**Pr.** Faiza KHELLAF	Université de USTHB
Examinateur	**Pr.** Khaled REZEG	Université de Biskra
Invitée	**Pr.** Malika IOUALALEN	Université de USTHB

2021/2022

“The way of success is the way of continuous pursuit of knowledge.”

Napoleon Hill

Acknowledgements

First and foremost, I would like to thank Almighty ALLAH, who gave me the strength, patience, and courage to continue this work.

My sincere gratitude goes to my supervisor, Pr. Okba KAZAR for multiple reasons that elevated the quality of this work: his patience, encouragement, advice, and especially the confidence he had in me.

I express all my gratitude to co-supervisor Pr. Laid KAHLOUL for his advice and support.

Also, I would like to warmly thank the jury. Starting with the president, Prof. Mohamed Tayeb LASKRI as well as the examiners: Prof. Faiza KHELLAF, Prof. Khaled REZEG, and Prof. Malika IOUALALEN for having done me the honor of accepting to judge this work, also generously offering their time, guidance, and goodwill throughout the review of this document.

Last and not least, I would like to thank all my teachers, friends, and colleagues in the computer science department.

Maroua Ahmid

Dedication

In my life, I love,

My sisters, brothers, and friends,

But, please excuse me,

There are two people that I want to mention

My mother, the source of happiness and motivation,

My father, the source of advice and patience,

To all of you, I dedicate this dissertation.

Maroua

الملخص

في السنوات الأخيرة، أصبحت إنترنت الأشياء (IoT) معروفتا كثيرًا. ولقد جذبت الكثير من الاهتمام بفضل تطبيقاتها القوية في مختلف المجالات. حاليًا، مليارات من أجهزة إنترنت الأشياء متصلة بالانترنت. يؤدي الارتفاع الهائل في عدد الأجهزة المتصلة إلى إنتاج المزيد من البيانات التي تتطلب تقنيات تخزين ومعالجة عالية. إلى جانب ذلك لدي معدات إنترنت الأشياء قدرة معالجة و التخزين محدودة لا تسمح بمعالجة البيانات أو حتى تخزينها. أيضا لا يمكن للأشياء اتخاذ قرارات ذكية وسريعة لتحقيق أهدافها، وتعتمد قدرة الشيء على التواصل مع أشياء أخرى على تشابه الخدمة وبروتوكولات الاتصال؛ سيؤثر ذلك على أداء تطبيقات إنترنت الأشياء وكفاءتها وتطويرها وقابليتها للتوسع. تقدم هذه الأطروحة ثلاث مساهمات رئيسية، في المساهمة ألأولى نقترح نهج Cloud-IoT لتوفير حل فعال لتخزين وتحليل البيانات الناتجة عن تطبيقات إنترنت الأشياء وتحسين قابلية توسعة إنترنت الأشياء. من أجل إثبات جدوى النهج المقترح تم تطوير نظام Cloud-IoTلمراقبة المريض عن بُعد.

أصبح أمن إنترنت الأشياء مشكلة أكثر صعوبة بسبب حدود الحوسبة والاتصالات لأجهزة إنترنت الأشياء مما يجعل إنترنت الأشياء أكثر عرضة لهجمات الأمن والخصوصية. و من ثم، كمساهمة ثانية، نقترح حلاً قويًا يعتمد على التشفير الخفيف لضمان أمن البيانات. أيضًا، استخدمنا آلية التحكم في الوصول لضمان خصوصية البيانات. توضح التجربة أن الحل المقترح أكثر ملاءمة لأجهزة إنترنت الأشياء .للاستفادة القصوى من تدفق البيانات ألضخمة يحتاج إنترنت الأشياء إلى إدارة وتحليل البيانات في الوقت الفعلي .من أجل تعزيز ذكاء أجهزة إنترنت الأشياء وتحسين نهجنا ألأول قمنا بتطوير حل فعال ومستقل يعتمد على الوكيل من اجل إدارة البيانات وتحليلها في الوقت الحقيقي كمساهمة ثالثة .يمكن للنظام المقترح اتخاذ قرارات سريعة و مناسبة في حالة الطوارئ.

الكلمات الرئيسية: إنترنت الأشياء ،الحوسبة السحابية ،نظام متعدد الوكلاء ،الأمن ،الرعاية الصحية والتشفير.

Résumé

Ces dernières années, l'Internet des Objets (IdO) est devenu très connu. Il a attiré beaucoup d'attention grâce à son application puissante dans les différents domaines. Actuellement, des milliards d'appareils IdO sont connectés. L'augmentation massive du nombre d'appareils connectés produit instantanément des données plus qui nécessitent technologie élevée de stockage et de traitement. Aussi, matériel IdO a une capacité de traitement et de stockage limité ne permet pas le traitement des données ou même le stockage. Également, les objets ne peuvent pas prendre des décisions intelligentes et rapides pour atteindre leurs objectifs, et la capacité de communication de l'objet avec d'autres objets dépend de la similarité des services et protocoles de communication; cela aura un impact sur les performances, l'efficacité, le développement et la scalabilité des applications IdO. Cette thèse propose trois contributions principales, dans la première contribution, nous proposons une approche Cloud-IdO pour fournir une solution efficace pour le stockage et l'analyse des données générées par les applications IdO et améliorer la scalabilité de l'IdO. Afin de démontrer la viabilité de l'approche proposée, un système Cloud-IdO pour la surveillance à distance des patients est développé.

La sécurité de l'IdO devient un problème plus difficile en raison des limites de calcul et de communication des appareils IdO qui rendent l'IdO plus vulnérable aux attaques de sécurité et de confidentialité. Ainsi, comme deuxième contribution, nous proposons une solution robuste basée sur une cryptographie légère pour assurer la sécurité des données. De plus, nous avons utilisé un mécanisme de contrôle d'accès pour garantir la confidentialité des données. L'expérimentation démontre que la solution proposée est plus appropriée aux appareils IdO. Pour tirer le meilleur parti des flux de données massifs, l'IdO a besoin d'une gestion et d'une analyse des données en temps réel. Afin de renforcer l'intelligence du dispositif IoT et d'améliorer notre première approche, nous avons développé une solution efficace, autonome basée sur les agents pour la gestion et d'analyse des données en temps réel, comme troisième contribution. Le système proposé peut prendre des décisions rapides et appropriées en cas d'urgence.

Mots clés: Internet des Objets, Cloud, Système Multi-Agents, Sécurité, Soins de Santé et Cryptographie.

Abstract

In recent years, the Internet of Things (IoT) has become well known. It has attracted much attention thanks to its powerful application in different fields. Currently, billions of IoT devices are connected. The massive rise in the number of connected devices instantly produces further data that requires high storage and processing technology. Besides, the IoT equipment has limited processing, and storage capability did not allow data processing or even storage. Also, things cannot make smart and quick decisions to achieve their goals, and the thing ability to communicate with other things depends on service similarity and communication protocols; this will impact the performance, efficiency, development, and scalability of IoT applications. This thesis provides three main contributions, in the first contribution, we propose a Cloud-IoT approach to provide an efficient solution for the storage and analysis of data generated by IoT applications and improve IoT scalability. In order to demonstrate the viability of the proposed approach, a Cloud-IoT system for remote patient monitoring is developed.

IoT security becomes a more challenging problem due to the computing and communication limits of IoT devices make IoT more vulnerable to security and privacy attacks. Hence, as a second contribution, we propose a robust solution based on lightweight cryptography to ensure data security. Also, we have used the access control mechanism to ensure data privacy. The experimentation demonstrates that the proposed solution more suitable for IoT devices. To tap the most out of massive data streams, IoT needs real-time management and analysis of data. In order to enhance the intelligence of IoT devices and to improve our first approach, we have developed an efficient, autonomous, and real-time solution based on the agent for data management and analysis as a third contribution. The proposed system can make fast and apt decisions in an emergency case.

Keywords: Internet of Things, Cloud, Multi-Agent System, Security, Healthcare, and Cryptography.

Table of Contents

List of Tables

List of Figures

List of Algorithms

List of Abbreviations

IoT	Internet of Things
MIT	Massachusetts Institute of Technology
MEMS	Micro-Electro-Mechanical Systems
CERP-IoT	Cluster European research projects on the Internet of things
NFC	Near Field Communication
GSM	Global System for Mobile Communications
LTE	Long Term Evolution
LoRa	Long Range
IIoT	Industrial Internet of Things
CO2	Carbon dioxide
G-IoT	Green Internet of Things
WSN	Wireless Sensor Network
DC	Data Center
QoS	Quality of Service
M2M	Machine-to-Machine
AI	Artificial Intelligence
ML	Machine Learning
NLP	Natural Language Processing
DL	Deep Learning
AIoT	Artificial Intelligence of Things
BMI	Body Mass Index
GPRS	General Packet Radio Service
CHF	Chronic Heart Failure

ECG	Electrocardiography
GSM	Global System for Mobile Communications
WBSN	Wireless Body Sensor Networks
IDE	Integrated Development Environment
SDK	Software Development Kit
WHO	World Health Organisation
BPM	Beats per Minute
MAC	Message Authentication Codes
DES	Data Encryption Standard
OCB mode	Offset codebook mode
AES	Advanced Encryption Standard
PKI	Public-Key Encryption
CP-ABE	Ciphertext-Policy Attribute-based Encryption
RSA	Rivest-Shamir-Adleman
MEMK	Memory Efficient Multi Key
CRT	Chinese Remainder Theorem
ECC ElGamal	Curves Cryptosystem ElGamal algorithm
UN	Username
Password	PW
NIST	National Institute of Standards and Technology
MAS	Multi-Agent Systems
DA	Device Agent
GA	Gateway Agent
WAN	Wide Area Network
PAN	Personal Area Network
LAN	Local Area Network

MA	Manager Agent
AA	Analyzer Agent
UA	User Agent
JADE	Java Agent DEvelopment Framework
GUI	Graphical User Interface

General Introduction

In the introduction of this thesis, we will first present the context and problematic of the research work, followed by an overview of the thesis's contributions. Finally, we will describe the thesis organization.

Context and Problematic

The Internet of Things is a new Internet revolution. It contributes connects the digital and the physical world by using information and communication technologies. It also provided powerful applications that permeating into practically all areas that play a leading role and directly affect the lives of humans, such as healthcare, industry, transportation, and logistics. IoT facilitating people's daily lives accelerated economic growth. However, many issues and challenges still represent significant concerns for IoT growth and development and widespread adoption. The IoT challenges are related to many factors, such as a heterogeneous environment, increased demands for data storage and processing, security and privacy threats, etc.

The huge increase of connected devices number generates more data immediately that requests for more storage and processing technologies. Total data volume for IoT devices worldwide is expected to exceed tens of zettabytes in the next few years, this will exacerbate the challenges of storing, processing, and managing large volumes of data. In addition, data security and privacy issues must be considered seriously in IoT applications due to the volume and the sensitivity of data created and distributed through the network, accessible not only by users but also by devices and services. Furthermore, the IoT device's limitations in terms of processing and storage make IoT more vulnerable to protection and privacy attacks. While the loT system shows capable of making decisions and interacting intelligently with its devices, the real situation is that these devices are still not smart enough to make quick and smart decisions in dangerous situations. It works so based on specific business rules and does not take into account unexpected environmental changes. Furthermore, the ability of devices to communicate with other devices is dependent on service similarity and contact protocols. Addressing

these problems would be the key to achieving the long-term efficiency and stability of IoT.

Contributions

In view of all the above problems, this thesis has three contributions; each of them addresses a particular issue:

- As the first contribution, a Cloud-IoT approach for real-time remote monitoring is proposed. We concentrate on the concept of integrating IoT and cloud computing technologies to enhance the IoT ability of processing and storage by the cloud's limitless power and capability, as well as to improve IoT scalability. In order to prove the feasibility of our approach, a Cloud-IoT system for remote heart rate monitoring is developed.
- As the second contribution, an integrated privacy protection system for IoT is proposed. The proposed system ensures data confidentiality in the perception layer and controls access to the data in the cloud.
- As the third contribution, a Cloud-IoT system based on smart agents is proposed, represent an integrated system that combines IoT and intelligent agent technology to enhance IoT intelligence. In order to prove the feasibility of our approach, a Cloud-IoT system based on smart agents for the health monitoring of cardiovascular patients is proposed. This approach conforms to the approaches proposed in the previous contribution.

Thesis Organization

This thesis is contained four chapters, organized in the "articles" format. So, some chapters are transcriptions of papers that have been published in or submitted to international journals and conferences.

- Chapter 1 gives an overview of the Internet of Things. Here, we provide definitions, characteristics, architecture, and applications of IoT. In addition, we highlight the most critical issues and challenges of IoT.

- In chapter 2, we propose a Cloud-IoT approach to improve IoT scalability. In order to prove the feasibility of the proposed system, a Cloud-IoT system for remote patient monitoring is developed. Also, we carry out the experimental analysis of the proposed approach.
- In chapter 3, we propose an integrated privacy protection system for IoT. In order to verify the efficiency of the proposed system, a study of the performances of the proposed approach is elaborated by experimentation.
- In chapter 4, we propose a Cloud-IoT system based on smart agents has been proposed. It represents an integrated system that combines IoT and intelligent agent technology to enhance IoT intelligence. We evaluate our proposal by experimentation.
- Finally, the thesis conclusion synthesizes the contributions and highlights the future perspectives of this research.

“The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so.”

Kevin Ashton

Chapter 1

Internet of Things Overview

1.1 Introduction

Over the past several years, many research have contributed to the emergence of the Internet of Things (IoT). In October 1989, John Romy developed a toaster that could be switched on/off from Internet, which was considered the first IoT device [1]. After one decade, the term Internet of Things was first used in 1999 by Kevin Ashton at the Massachusetts Institute of Technology (MIT) [2]. Over several years, the Internet of Things evolved due to the integration of different technologies, ranging from cellular networking to the Internet and from embedded devices to micro-electromechanical systems (MEMS) [3], which leads to increase the number of devices, for the first time, the number of devices connected to the Internet outnumbered the number of people in the world in 2008 [4]. In recent years, IoT research has become very popular and has attracted much attention from research teams. It contributed to interconnecting the physical world and the virtual world by using multiple information and communication technologies. It also provided powerful applications and systems in different fields, including healthcare, industry, transportation, and logistics. Consequently, it facilitated people's daily lives and accelerated economic growth. However, IoT technology is still facing several issues that need to be addressed.

For more understanding IoT, the present chapter provides an overview of the Internet of Things. It introduces the different definitions and characteristics of IoT, describes the architecture of IoT and explains its layers, and most useful IoT applications fields, also highlight the most critical issues and challenges.

1.2 IoT Definitions

The Internet of Things is a new Internet revolution; it connects the digital and the physical world. The IoT allows things to connect everything and anyone, at any time, anywhere, using any network. As shown in Figure. 1.1. It has introduced a new dimension to information and communication technologies, in addition to the time, space, and network dimensions that allow anybody to connect at any time and from anywhere, through any network. Now we have a new thing dimension that allows us to connect to anything can be tagged, monitored, and connected.

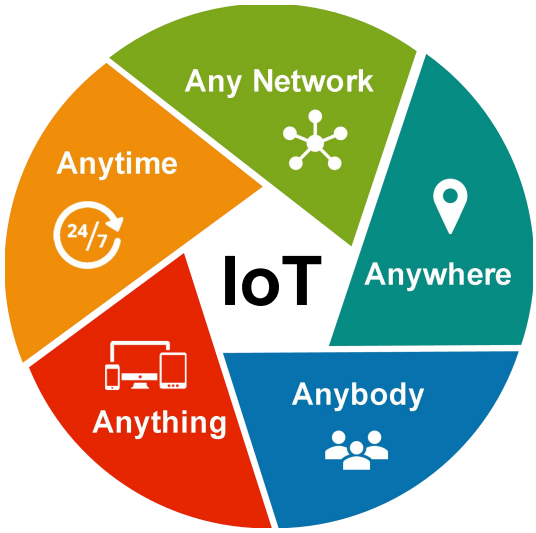

Figure 1.1. Internet of things dimensions.

1.2.1 Internet of Things

Since coined IoT term for the first time, attempts have been made to define the Internet of Things by many different groups, including researchers, academicians, developers, and corporate people. However, until now, there is no universal definition of the Internet of Things. In the following, we mention the most known definitions of the Internet of things.

Haller, Karnouskos and Schroth define the Internet of Things as "A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are

available to interact with these smart objects over the Internet, query their state and any information associated with them, taking into account security and privacy issues." [5]

The Cluster European research projects on the Internet of things (CERP-IoT) defines the Internet of things as: "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network." [6]

1.2.1 Thing

A thing in the context of IoT is a physical device with a unique identifier associated with at least one address that can be machine-readable and used to communicate with it. It has an embedded system, has at least one communication model shown in Figure 1.2, some essential computing skills; this can range from the ability to sensing to the ability to perform complex calculations. It role is to detect physical phenomena (temperature, light, level of electromagnetic radiation, etc.) from the physical environment around them by using embedded sensors, collect data, then sent it to the desired destination through the Internet. Also, it may have the ability to act or react in the face of situations and changes in the environment.

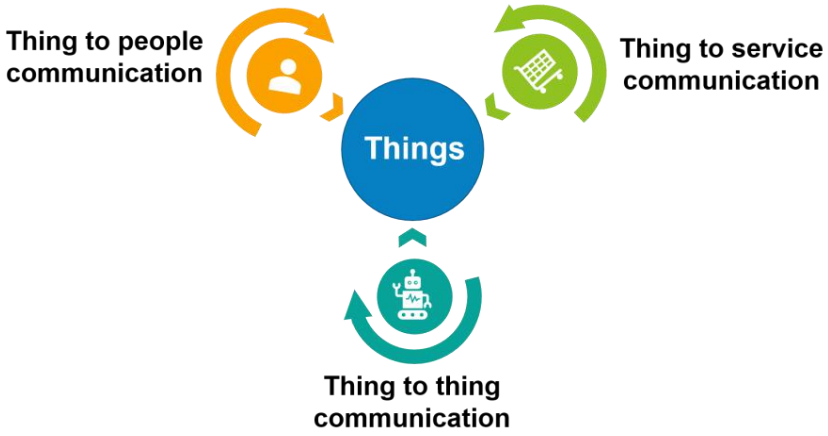

Figure 1.2. Communication models in IoT.

1.3 IoT Characteristics

The IoT has several characteristics; those characteristics differ depending on the domain. In the following, some of the common fundamental characteristics of the IoT.

1.3.1 Connectivity

In the IoT system, devices, services, and even people connected to the Internet, to collect, store and exchange the data that will be analyzed later. The connection of IoT devices is pivotal as these simple interactions contribute to the collective intelligence of the IoT system. Each IoT system has specific needs that determine the most suitable connectivity technology. The choice of connectivity technology depends on different elements, such as the application domain, network type, distance, and the environment, etc [7].

1.3.2 Heterogeneity

Heterogeneous IoT refers to allow communicating with a wide variety of devices using multiple protocols. Today, there is a large collection of different IoT devices. and applications that interact with other devices, services, or platforms through various kinds of networks [8]. Heterogeneity is an important feature of the IoT system as it enhances IoT scalability, but at the same time, managing a huge number of heterogeneous devices is a big challenge.

1.3.3 Dynamic Nature

IoT dynamic nature means any changes in devices state such as connected/disconnected, location, speed, etc. Also, any change around the device [9], such as a change in temperature and humidity degree, or even a change in the number of devices by connecting new things and applications, disconnecting others, add new services, segregate services, discontinue services, etc. IoT technology is constantly evolving and progressing at a fast pace.

1.3.4 Enormous Scale

Internet-connected devices are increasing day by day. For the first time, the number of Internet-connected devices outnumbered the world's population in 2008 [4], with their number reached 7 billion devices in 2018. By 2022, Cisco visual networking index expects that 12.3 billion devices will be connected to the Internet, exceeding the world's projected population at that time (8 billion) by 4.3 billion devices [10]. Thus, management, analysis, and interpretation of the generated data will become more challenging.

1.4 IoT Architecture

The IoT has special characteristics that must take into consideration when designing the IoT architecture; for this reason, many researchers have proposed various architectures for IoT with three layers, four layers, and five layers [11]. The most popular and widely applied model is four-layer architecture [12] as shown in Figure 1.3.

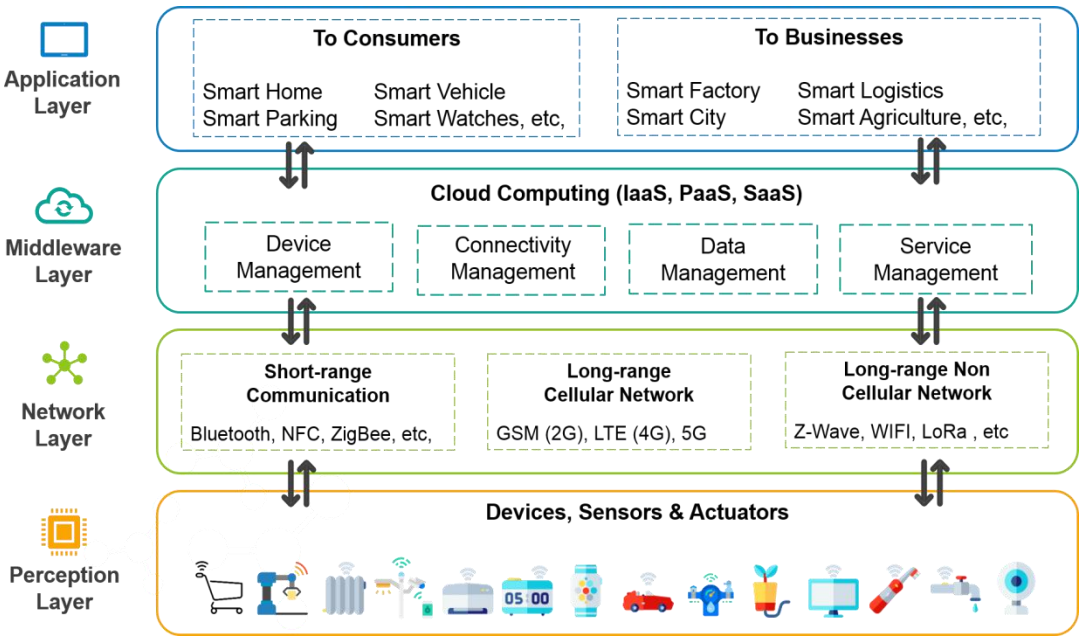

Figure 1.3. Internet of things architecture.

1.4.1 Perception Layer

The perception layer or "device layer" represents the bottom layer of the Internet of things architecture, consisting of different sensors, actuators, and real-world objects [13]. The perception layer's primary responsibilities are to measure, detect, collect, and extract data related to devices. This data may be related to the object's location, movement, and direction or related to environmental factors such as humidity, temperature, and wind speed, etc.

1.4.2 Network Layer

The network layer or "transmission layer" plays an essential role in transferring the information collected from sensors to the middleware layer's processing unit, in addition to addressing, and routing functions [13]. Its principal goal is to connect all things together and allow things to share the data with other connected things via the Internet [14].

1.4.3 Middleware Layer

The primary responsibility of the middleware layer or "service layer" is the service configuration and management. Also, determine the most appropriate service or device to satisfy the user request, because IoT devices can implement specific services and can only connect and communicate with those that implement the same type of service [15]. Moreover, the middleware layer aggregate, filter, save, process, and analyze the data coming from the network layer then make decisions [16].

1.4.4 Application Layer

The application layer is the highest layer in IoT architecture, and it is visible to the end-user. Mainly it managing the applications based on the data managed and treated by the middleware layer, also, supports the service requests by users [17]. It includes all applications using IoT technology; it can be healthcare, manufacturing, and transportation, etc.

1.5 IoT Applications

The goal of IoT is to increase the efficiency of the environment in order to make them more profitable and comfortable for people; IoT solutions can provide competitive advantages over current solutions. Currently, there are numerous and diverse IoT applications, permeating into practically all areas that play a leading role and directly affect the lives of humans. According to the IoT analytics research tracking IoT platforms, the most IoT projects in 2020 were developed in manufacturing, industrial, transportation, energy, retail, cities and healthcare as shown in Figure 1.4, where the analysis was based in 1414 actual IoT projects.

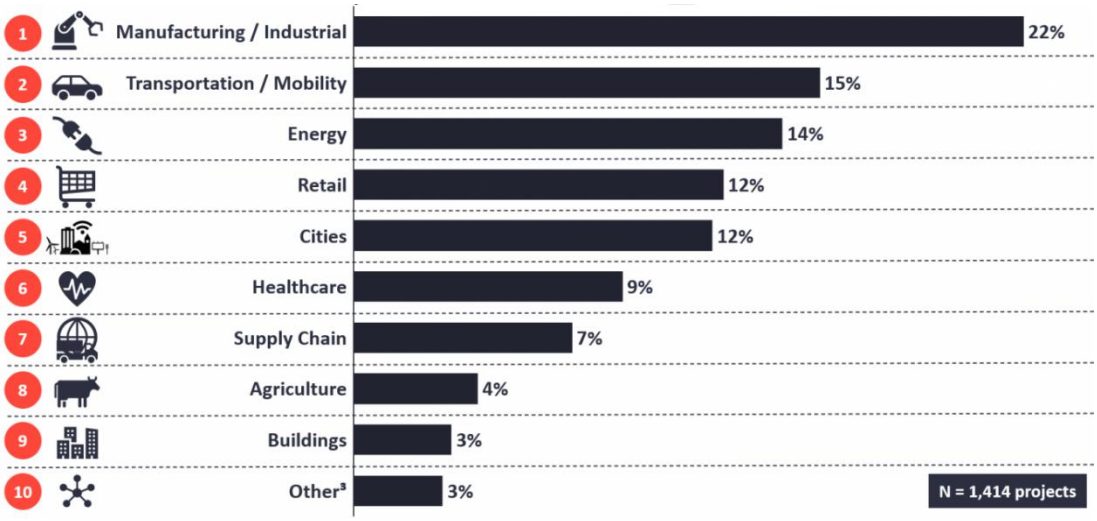

Figure 1.4. Top 10 IoT projects in 2020 [60].

1.5.1 Healthcare

In the healthcare field, IoT has gained more attention because of its vital role in this field. It moves the medical process away from hospitals and provides patients the ability to access care remotely and receive assistance in emergency cases. It also allows healthcare providers to monitor patient health status in real-time, at home, work, or anywhere [18]. The real-time monitoring system helps healthcare professionals to understand the variations that can influence patients' health status and help them detect illness early. Also, it may reduce complications and help the healthcare providers propose the appropriate treatment before things go wrong [19]. Thus, save patients' lives.

Moreover, IoT improves the quality and effectiveness of service at a lower cost and improves patients' lifestyle and supports independent or semi-autonomous living, especially in the case of the elderly, disabled, or people who have a chronic illness requiring constant supervision.

The advance in sensor technology, including wearable, implantable, and ambient sensors, allows healthcare providers to monitor patient health status and vital information such as heart rate, temperature, oxygen saturation, etc. Healthcare application growth is growing in tandem with the advancement in sensor technologies [20]. There are currently various healthcare applications such as mood monitoring, oxygen saturation monitoring, human activity recognition, etc. One of the most promising applications is a small sensor shown in Figure 1.5, that sticks to a person's throat and detects heart rate, body temperature, measuring the vibrations of coughs and chest movements for detecting early signs of COVID-19 symptoms.

Figure 1.5. The COVID-19 symptoms sensor [21].

1.5.2 Industrial

The Industrial Internet of Things (IIoT), known as the fourth industrial revolution (Industry 4.0) [22], shapes the future of innovative and modern manufacturing. It aims to automate the cycle of manufacturing from material warehousing to marketing. IIoT facilitates the production flow in a manufacturing plant, helps stakeholders monitor the supply chain, manages warehouses. IIoT gives industrial managers a more accurate view of how industrial operations are moving along and find dark places in the manufacturing

process such as defects in machinery, or a machine goes down [29]. Also, help them monitor the factors that might lead to operating conditions that are less than optimal and make informed business decisions to improve productivity, thus providing faster time to market and increase profits [23].

Today, with the advancement of IIoT, several IIoT applications already on the market. One of them is YuMi robot, it is a dual-arm robot with work side-by-side with people on the same tasks, and it is tireless the precise and repetitive tasks such as small parts assembly, as shown in Figure 1.6.

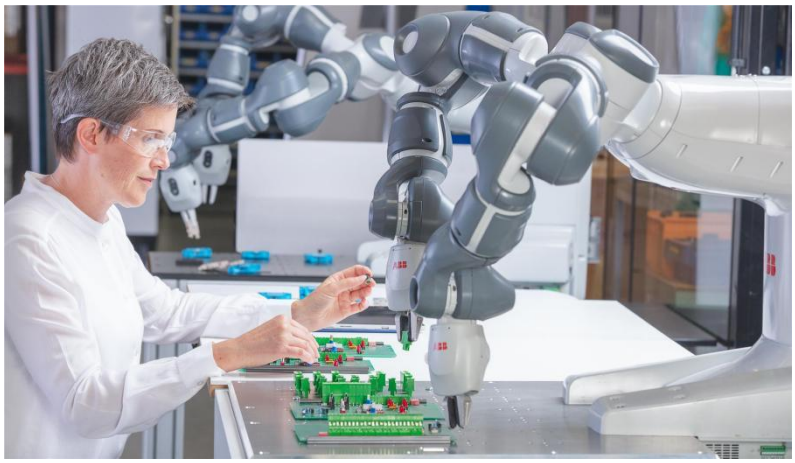

Figure 1.6. The YuMi dual-arm robot [24].

1.5.3 Transportation

Transportation is the backbone of our lives, and the need for it is increasing day by day. Thus, transportation must be improved not only for passenger safety and security but also for the goods transported and vehicles. Currently, IoT makes a revolution in the transportation industry and makes transportation safer by integrating sensors in roads [25], railways, and vehicles will lessen the chances of sudden breakdowns and helps to predict the possible failures of the machine parts, also help the maintenance department for the preventive measures. As a result, lesser maintenance breakdown delays. Also, IoT allows better monitoring and analysis of traffic flow through devices at all traffic observation points; it helps drivers with suggestions of alternative roads in case congestion, helps them get parking spots, and informs them of the fees required [26]. They are thus leading

to minimize traffic congestion and improve road safety. Now, there are many IoT applications in transport, such as real-time location monitoring of the fleet, tracking of cargo, fuel and mileage statistics, smart cars, etc.

BMW i8 sports car shown in Figure 1.7 is equipped with several sensors. These sensors collect a set of data such as location, mileage, destination routing, battery voltage, fuel, and fluid levels, in addition to the health and status of the car components, etc. Soon, it will also pick up more weather data through sensors on the vehicle. This data is available to drivers through the BMW Connect app, which provides time-to-leave notifications, car remote control, monitoring, etc.

Figure 1.7. BMW i8 sports car.

1.5.4 Cities

A smart city is a city connected, equipped with a significant number of sensors and actuators, this enables it to track, monitor, manage, and control the city. Also, it accurately identifies the points that need improvement and implements most of the changes remotely, to anticipate any anomalies and improve the quality of life for citizens [26]. Smart cities applications can make cities more effective and efficient. It provides efficient management of waste, water supply, and energy to reduce economic and environmental costs [27], fast assistance in emergency cases due to surveillance systems anywhere, etc. As shown in Figure 1.8, there are many IoT applications in smart cities such as the smart grid, smart governance, smart education, and smart buildings, etc [28]. In the last few years, various smart city projects have been launched, such as Oslo, San

Francisco, London, Barcelona, and Singapore. In 2018 Algerian government started an ambitious project to transform Algiers city into a smart city by 2035 gradually.

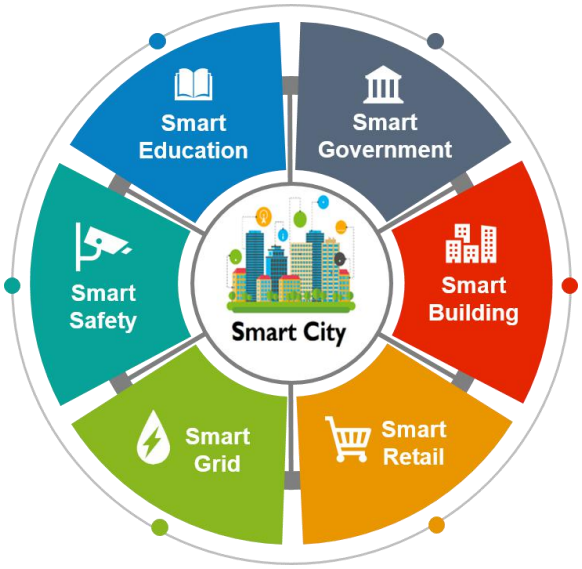

Figure 1.8. Smart city applications.

1.6 Challenges and Issues

IoT affects various aspects of human lives, as we mentioned in the previous section. However, many issues and challenges still represent significant concerns for IoT growth and development and widespread adoption. Therefore, problems and concerns related to IoT need to be addressed from different aspects, such as services, social and environmental impacts, etc [30]. The IoT challenges are related to many factors, such as a heterogeneous environment, increased demands for data storage and processing, security and privacy threats, etc., overcoming them will be the key to creating lasting productivity and prosperity.

1.6.1 Green IoT

The rapid IoT growth accompanies further deterioration of the environment resulted in high energy consumption, the accelerated exhaustion of traditional energy resources, waste, the greenhouse effects, carbon dioxide (CO2) emissions, etc. Therefore,

there is a need to minimize the negative influence of IoT technology on the environment and reduce the implementation resources of applications and to make sustainable IoT, a green Internet of Things (G-IoT) is proposed [31]. The responsibility lies in the hands of the system engineer and designer to design, program, and configure the IoT devices, services, and applications in the most sustainable way [32]. In the following, we will explain the critical points of green IoT shown in Figure 1.9.

- A wireless sensor network (WSN) consists of many sensor nodes with limited power, powered by the battery. In some cases, a low power level may not be determined until a very late stage. At this point, the node or the entire WSN crashes due to failure to meet power requirements [33], because of high power consumption and the daily need to replace the battery has made WSN challenging and costly to maintain. There is a need to save energy consumption by using renewable energy mechanisms for charging and utilization purposes and generating energy from environmental elements [34] such as vibrations, kinetic, sun, etc.

- With growing application utilization of cloud, more data center (DC) needs to be deployed, thus more power consumption, energy dissipation in the environment by these DC, and carbon footprints [35]. Moreover, continuous use of processor chips produces more heat, more heat requires cooling, and the cooling process produces heat again. There is an important need to develop software solutions consuming less energy with minimum resource utilization with high quality of service (QoS) [36]. Also, design and manufacture devices that consume less energy with the same computing speed.

- The machine-to-machine (M2M) technology involves a large number of machines communicating and sharing information with us; the M2M communication paradigm supports a variety of IoT applications, especially real-time monitoring applications. However, the vast number of massive machines involved in M2M communications will consume much energy [37].

- Today, the economy, energy, and environment gain much attention, with a particular focus on keywords like sustainability and environment friendly for creating a greener start for the future [38]. Renewable alternatives such as hydro, solar, and wind energy

will gradually be the major resource of energy in the future [39], to meet growing energy demands and mitigating climate change.

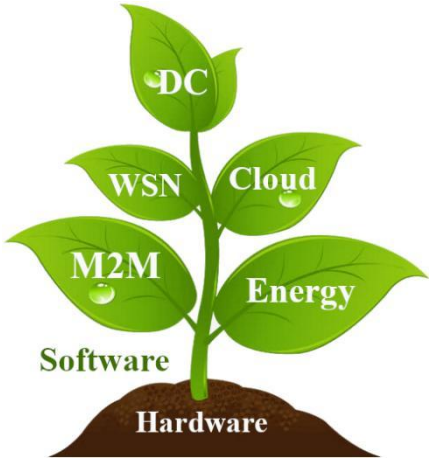

Figure 1.9. The green Internet of things.

1.6.2 Security

Security and privacy become more critical and challenging; they must be considered seriously in IoT due to the quantity and the sensitivity of data created and distributed through the network, accessibility to it not only by users but also by devices and services [40]. Also, the computing and communication limits of IoT devices make IoT more vulnerable to security and privacy attacks; this problem is further compounded by the exponential growth of the number of connected devices. According to the HP company report, nearly 70% of IoT devices are exposed to attacks and violations [41]. Numerous security threats exist on each layer in IoT architecture that must be addressed appropriately to avoid causing damage. As shown in Figure 1.10, each IoT layer has its security requirements that must be ensured at each level of IoT architecture to implement a completely secure IoT system [42]. In the following, we will briefly explain the key security threats of each IoT layer:

- The most devices in the perception layer are usually worked in outside environments, which facilitates the tamping with hardware components, change the measurements, shapes, or mechanical properties of these parts. The wireless network is the most used in this layer, which makes it easily penetrated through disturbing waves [43]; thus, the

attackers can control the devices and catch all the data, send malicious data, or even compromising the confidentiality of information [42].

- The attacker can penetrate privacy and confidentiality in the network layer by eavesdropping, surveillance, and traffic information analysis. Also, he can get unapproved access to IoT devices, and modifying critical data values utilize it for criminal goals [44]. The attacks may be external attacks by people from outside of the network, they do not have access permission to IoT network or even internal attacks by people who have permission and privileges to enter the network and they use it illegally [42].
- The most security problems facing the middleware layer are in cloud computing due to the data centralization, like loss of subtle data, data escape, cloning, intercept data-in-motion, and moves data ownership [45]. Therefore, individuals and service providers lose control over sensitive data. Also, breaching the security of any component in the virtual infrastructure affects the security of other components and, thus, affects the overall system security [46], [47], thus resulting in personal, and financial harm.
- Like the other layers, there are many security challenges related to the application layer, especially access control and privacy challenges, where every application has many users with varying degrees of access privileges. Also, various applications with different authentication mechanisms, making it extremely difficult to merge them all [48]. The privacy challenges are related to the data volume that will be uncovered, who, and when to use it [49].

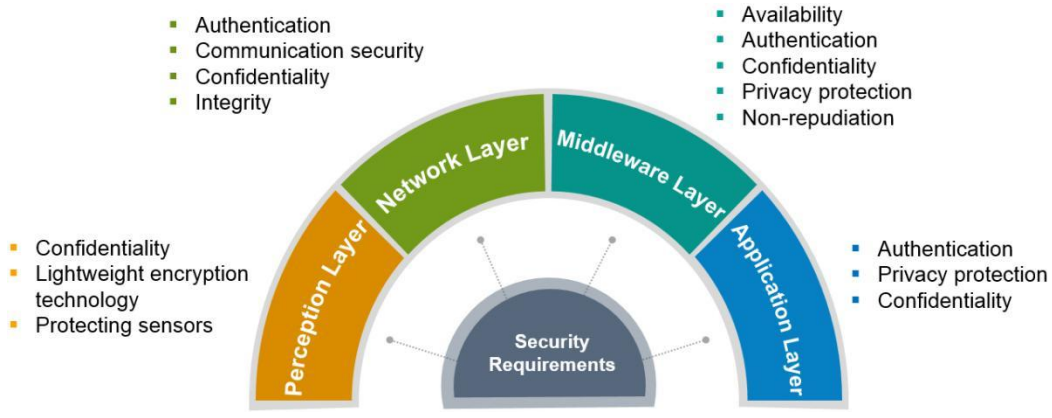

Figure 1.10. Security requirements of each IoT layer.

1.6.3 Data Storage and Processing

According to Statista research department, the total data volume of IoT devices worldwide is projected to exceed 79.4 zettabytes by 2022 [61]. The huge increase of connected devices number generates more data immediately that requests for more storage and processing technologies, this makes the combination of cloud and IoT has become inevitable to enhance the IoT ability of storage and processing with unlimited capabilities and resources of the cloud [50]. IoT and cloud integration offers new possibilities for the development of IoT applications. However, various challenges arise during the storage, processing, and management of massive amounts of data in cloud environments.

In IoT data storage, the key problems are the transferring and isolating of data within the cloud platform. In most cloud platforms, different tenants share the same computing resources for improving the utilization of cloud resources; this may cause a difference in data authority and require data isolation in the cloud platform [51]. Another issue, transferring massive data from edge devices to the cloud infrastructure causes certain network performance problems such as delays, congestion, availability, etc. Also, the costs of transferring data over the Internet and storing data on cloud servers [52].

The heterogeneity is one of the IoT characteristics. At the same time, it is a challenge to integrate massive heterogeneous data from multiple devices with different types of structured, semi-structured, and unstructured data that should be processed and integrated to create a comprehensive and meaningful view for further utilities. However, the oversimplification of data could lead to unfounded conclusions [53]. Traditional sequential pattern algorithms can pose the challenge of scalability when working with big data. On the other hand, the current parallel systems in the cloud are incapable of effectively supporting complex parallel processing. Furthermore, high costs, and lack of interaction ability in real-time processing [54].

1.6.4 Intelligence

While the loT system shows the ability to make decisions and interact smartly between the devices, it does so based on specific business rules without considering unintended environmental changes [55]. Also, things cannot make smart and quick decisions to achieve their goals and the thing ability to communicate with other things depends on service similarity and communication protocols [56]. As we mentioned before, IoT devices produce massive data streams with varied data sources and types, changes continuously. To tap the most out of this overwhelming these data, IoT needs real-time management and analysis of data and create accurate insights from these data; this will challenge the data management and analysis capability of IoT.

The use of autonomous technologies such as artificial intelligence (AI), makes IoT more intelligent. From a technological point of view, AI is composed of a set of technologies such as and deep learning (DL), machine learning (ML), natural language processing (NLP). While IoT allows devices to interact via the Internet, AI lets them learn from their data and experience. AI allows companies to analyze and wring insights from data quickly, better interpret data, respond to events more rapidly in the case of a risk, mishap or failure, and make decisions similar to how a human brain does the same [57]. The use of AI they can avoid these failures in the first instance by using IoT-based predictive analytics to predict which the conditions result in failure of the devices in an automated manner without human intervention [58]. As a result, preventive action can be taken in time, thus avoiding costly repairs and avoid setbacks in their business. More to the point, increasing operational efficiency, save on unnecessary expenses, and making huge profits.

The combination of IoT and AI technologies together build a new concept to IoT, it is the artificial intelligence of things (AIoT) where IoT devices are the digital nervous system and AI is the brain of the system. As shown in Figure 1.11, AI with the cloud and big data technologies can make IoT applications realize their full potential when devices can analyze data, make decisions, and act on that data without humans' interaction [59]. Soon, it will be rare to find an IoT application that does not use AI in any way.

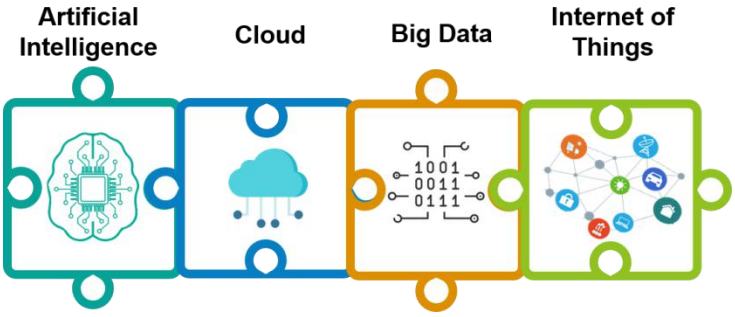

Figure 1.11. The requires technologies for Intelligent Internet of Things.

1.7 Conclusion

The Internet of things has changed the world; where it has introduced new dimensions to information and communication technologies that enable the connection to anything and interconnect the physical world and the virtual world. With the Internet of Things expanding every day, soon everything will be linked to the Internet. Moreover, it provided powerful applications and systems in different fields; that facilitated people's daily lives and accelerated economic growth, including healthcare, industry, and transportation, etc.

In order to understand the context of work, the presented chapter provides an overview of the Internet of Things. An introduction presents the evolution of embedded systems, information, and communication technology towards the new paradigm IoT over several years. The different definitions and characteristics of IoT are covered. Then, a detailed explanation of IoT architecture and its layers. Currently, there are numerous and diverse IoT applications, permeating into practically all areas, we have selected the most useful fields, that profoundly affect human lives. Since their unique characteristics pose new problems, we have highlighted the most critical issues and challenges.

“I believe, if you zoom out into the future, and you look back, and you ask the question, ‘What was Apple’s greatest contribution to mankind?’ it will be about health.”

Tim Cook

Chapter 2

A Cloud-IoT System for Remote Patient Monitoring

2.1 Introduction

According to the Statista Research Department, by 2025, 75.44 billion IoT devices will be connected [62]. The massive rise in the number of connected devices instantly produces further data that requires more storage and processing technology. Currently, IoT is one of the main big data sources. However, IoT devices have limited storage and processing capacities that do not enable on-site data storage and processing; this can impact IoT application development and scalability. Where the collection, storage, and processing of data will generate new challenges regarding performance and efficiency [6, 9]. For these reasons, special attention must be given to the storage, analysis, and access of the vast amount of generated data. Especially in the healthcare field, that requiring real-time analysis of vital patient data as a critical necessity to identify abnormal conditions, avoid possible illnesses, and act as fast as possible to save lives [63]. In terms of processing and storage capacity, the cloud has unlimited capacities. Also, cloud computing provides ubiquitous access to storage and computing power [64]. The combination of IoT and cloud will provide an efficient solution for the storage and analyses of data generated by IoT applications [65]. Considering all the above issues, this chapter aims to propose a Cloud-IoT approach to improve IoT scalability. In order to prove the feasibility of the proposed approach, a Cloud-IoT system for remote patient monitoring is developed.

The remainder of the chapter is organized as follows: Section 2.2 presents and discusses the related works. Section 2.3 presents the details of the proposed approach. Section 2.4 presents the experimental results. Section 2.5 concludes this chapter.

2.2 Related Works

The rapid growth of IoT applications in different fields leads to create a large amount of information. However, the IoT equipment has limited processing, and storage capability didn't permit field data processing or even storage. Thus, the collection, acquisition, processing, sharing, searching operation for large amounts of data represents a big challenge. The combination of IoT and cloud computing is desperately required to take advantage of almost infinite cloud capacity and resources to overcome technological constraints and to provide new services in a wide variety of real-life scenarios. However, previous research focuses mostly on the individual development of a single technique.

Recently, several authors [66–78] have proposed health monitoring systems. In [66], the authors developed an android application and IoT device for monitoring the pulse rate and Body Mass Index (BMI). The authors of [67] developed a wearable device for monitoring the blood oxygen saturation and heart rate of athletes. This device can send the data to the coaches and doctors via General Packet Radio Service (GPRS) and WiFi networks to provide them with the athlete's condition. In another work [73], the authors proposed a smartphone-based system for monitoring physical activity of patients with chronic heart failure (CHF), then send the collected data to a central server. In [68] project, the developed device can monitor a patient's pulse and body temperature, then transfer the data to a smartphone application. The proposed system in [69] can monitor electrocardiography (ECG), heartbeat, and temperature parameters. Then it sends results to the server via the Global System for Mobile Communications (GSM), then the doctors can observe the results on the website. Similar work to this work was proposed in [70]. In [71], the authors developed a heart monitoring system that provides an interface between the doctor and the patients for two-way communication. In [77], the authors proposed a smartphone-integrated ECG monitoring system that monitors the ECG of users during smartphone utilization. In [74], the authors developed a device that can measure the physiological parameters of the human body. The results are displayed directly on the Smartphone and used Bluetooth as wireless serial communication. In [78], the authors developed a wearable device for monitoring the heart rate and temperature of the human body. Then stores the results in a computer.

The proposed monitoring system in [72] uses wireless body sensor networks (WBSN) to sense the blood pressure and heart rate. It consists of multiple wireless relay nodes that transfer the data sent by the coordinator to the base station. In [75], the authors developed a personal health monitor for psychophysiological evaluation. The proposed system measures the heart rate variability through WBSN to quantify stress levels before and during intense training sessions of military members. In [76], the authors developed a health monitoring system based on a wearable device for monitoring the electrocardiogram, respiration, and activity, then send all signals to the remote monitoring center.

In the last few years, much research has been proposed for monitoring farms. In [80], the authors proposed an agriculture monitoring system based on WSN for monitoring the environmental factors and soil properties continuously such as moisture, temperature, and leaf wetness. In [81], the authors developed an automatic agriculture system based on a remote-controlled robot for doing agriculture tasks such as weeding, moisture sensing, irrigation, spraying, bird and animal scarring.. In [84], the authors proposed a farming system that measures the physical parameters such as soil moisture content, pH of the soil and nutrient content, for irrigator control, the quantity of green manure, and compost. The proposed system farmer to control the farming through the mobile phone. In [85], the authors developed an automatic irrigation system for controlling irrigation via the smartphone. The proposed system contains a portable device that measures soil moisture, air humidity, and air temperature, embedded into the irrigation system. For smart homes, several systems have been proposed for monitoring and control homes. In [79] project, the authors developed a smart home monitoring system for the elderly. They named (SEHMS) to help the elderly and individuals with disabilities live independently in their homes. In [82], the authors proposed a home lighting control system based on a smartphone. In [83], the authors designed a home automation system that allows old aged people to monitor and control the home via the android application.

Although several studies have developed monitoring systems in vital fields, little attention has been given to storage and analysis data issues that require the utilization of hug storage and processing resources. Knowing that IoT devices have limited storage and

processing capacity, that prevent on-site data processing and storage. Consequential issues of performance, security, and privacy will therefore affect the future development of applications. Also, scalability is a big challenge without sufficient infrastructure. Some previous studies support remote monitoring by using GSM and GPRS technologies. However, the problem with those approaches is that they are not providing real-time monitoring, GSM can only use SMS to transmit data. GPRS can send and receive short message service texts over the network, and it is data traffic speed is far greater than the GSM mode. However, it is not in real-time, and it is slower compared to wifi. Additionally, connecting to a mobile network consumes more battery life than connecting the mobile devices to a wireless network. Those approaches may not be practical in all situations, especially in critical cases that need real-time monitoring.

For these purposes, the present chapter aims to propose a Cloud-IoT approach for real-time remote monitoring. In order to verify the validity of the proposed approach, we developed a Cloud-IoT system for remote patient monitoring. It can be an effective way to benefit from limitless cloud capacities in terms of storage and processing power and improve IoT scalability and performance. Also, deliver real-life IoT-based services in a distributed, dynamic, and responsive manner. Also, handle a wide range of connections from millions of devices for enabling pervasive and ubiquitous computing scenarios.

Table 2.1 illustrates the differences between our work and the previously listed works from the aspect of the application area, communication technology, mobile application, support remote monitoring, and cloud. Also, it helps to identify the different technologies used to address the same issues.

Table 2.1. Comparison of IoT-based systems.

Refernece	Date	Application area	Communication technology	Mobile application	Support remote monitoring	Cloud
[66]	2018	Healthcare	Wi-Fi	Yes	No	No
[67]	2015	Healthcare	GPRS/ WiFi/ Zigbee	No	Yes	No
[68]	2017	Healthcare	Wi-Fi	Yes	No	No
[69]	2016	Healthcare	GSM	No	Yes	No
[70]	2016	Healthcare	GSM	No	Yes	No
[71]	2015	Healthcare	WiFi	Yes	Yes	No
[72]	2015	Healthcare	WiFi	No	Yes	No
[73]	2015	Healthcare	/	No	Yes	No
[74]	2019	Healthcare	Bluetooth	Yes	No	No
[75]	2003	Healthcare	Bluetooth	No	No	No
[76]	2005	Healthcare	GPRS	No	Yes	No
[77]	2016	Healthcare	Bluetooth	Yes	No	No
[78]	2012	Healthcare	/	No	No	No
[79]	2013	Smart home	Wi-Fi	No	Yes	No
[80]	2017	Smart agriculture	Wi-Fi	Yes	Yes	No
[81]	2016	Smart agriculture	Wi-Fi	No	Yes	No
[82]	2013	Smart home	Bluetooth	Yes	No	No
[83]	2013	Smart home	Bluetooth	Yes	No	No
[84]	2015	Smart agriculture	GSM	No	Yes	No
[85]	2014	Smart agriculture	Wi-Fi	Yes	Yes	No

2.3 System Architecture

Currently, millions of devices are connected now and are forecast to increase dramatically in the coming years, this number of devices needs a massive storage capacity. Also, the huge increase of connected devices number generates more data immediately, which requests for more storage and processing technologies that are not provided in IoT devices, this will generate many problems regarding performance and efficiency. Thus, it will impact IoT application development and scalability. In contrast, the cloud has unlimited resources and capabilities of processing and storage. Also, it provides and manages services at any time and everywhere with minimal management effort and expense. Moreover, it has many advantages, such as flexibility, high reliability, virtualization, high automation, high efficiency, scalability, low cost, and fast service providing.

For this purpose, we focus on the idea of integration between IoT and cloud computing technology to enhance the IoT ability of processing and storage with unlimited resources and capabilities of the cloud also improve IoT scalability, we propose a new hybrid solution to address the increasing demands for data storage and processing. As shown in Figure 2.1, the proposed system architecture is mainly composed of four components.

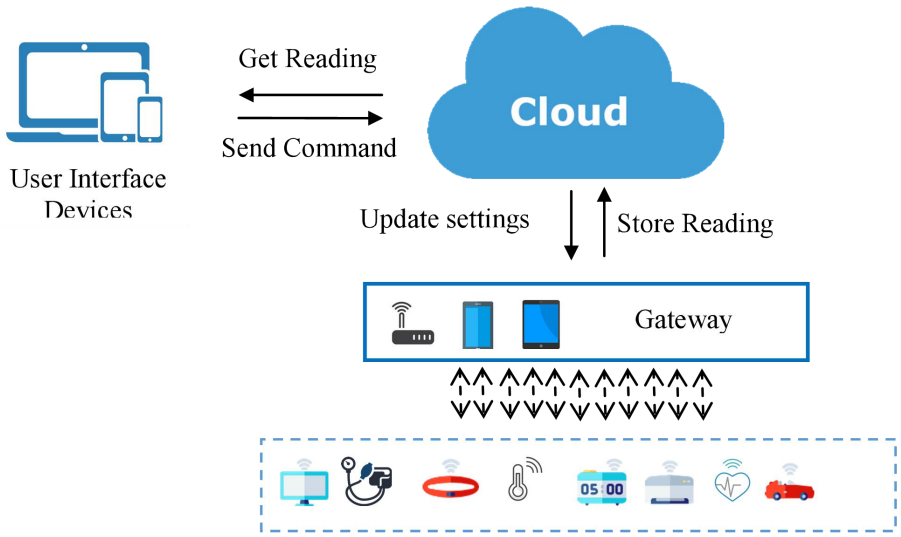

Figure 2.1. The general architecture of the proposed system.

2.3.1 Devices

Sensors and actuators can be purely integrated with devices or even attached to devices, machines, or items that have support for internet connectivity, in order to observe the physical world, measure the different surroundings factors, such as temperature, humidity, speed, etc., then transmit data over the internet or other networks. IoT devices can also be managed and controlled remotely when required. There are two possibilities, the data gathered from IoT devices will be sent first to the gateway then to the cloud, or sent it directly to the cloud, this depending on IoT communication capability.

2.3.2 Gateway

The gateway works as a communication point between various IoT devices and the cloud; it can be a smartphone, a router, a computer, etc. All data that moves to the cloud or vice versa will pass through the gateway if the device cannot connect directly to the Internet. Its key responsibilities are data collection and pre-processing, and uploading only the necessary data to the cloud in order to reduce the network traffic.

2.3.3 Cloud

The cloud server receives data from the IoT gateway (or IoT devices) and stores the data into the cloud database. The cloud providers are responsible for providing and managing computational and storage resources. They are also responsible for the accessibility to data from anywhere at any time and served data to several customers at a time. Thanks to the cloud, the users can monitor and/or control IoT devices from anywhere at any time via an application.

2.3.4 Application

The application can be a mobile application and/or web application. For ease of remote management of monitoring systems and remotely control the IoT devices, we have developed a mobile application updated in real-time and provides a visualization of

the sensor data to allow users to stay up-to-date 24/7 with the environment and device status.

2.4 Implementation and Results

In order to demonstrate the efficiency of the proposed system, the implementation of the proposed solution follows a series of steps to achieve a system capable of solving the problems posed in this chapter. The following shows the development tools, the configuration used to develop this system, the case study, system interfaces, and the experimental results.

2.4.1 Development Tools

We have used a set of hardware and software development tools to build our IoT healthcare solution.

- Android studio: is Google proprietary Integrated Development Environment (IDE) for Android application development, launched in 2013. It is based on IntelliJ powerful code editor and developer tools, free, available for Windows, Mac OSX, and Linux. Android Studio offers powerful features such as a raft of tools and Software Development Kit (SDK) for testing, debugging, and integrating with other SDKs, Built-in support for Google Cloud Platfor, and flexible Gradle-based build system [88].
- Firebase: is a set of hosting services for different types of applications. Launched in 2011 under the name Envolve, and was acquired by Google in October 2014. Firebase offers useful features for developing high-quality applications and extending the user base, such as real-time databases where firebase programs remain responsive even when offline; when connectivity is restored, the client computer receives any changes it has missed and automatically syncs with the new server status. Also, the application can be run by millions of users at the same time without encountering any bugs or losing responsiveness. Besides, it allows the developer the flexibility to upload and download files directly from clients via the Firebase SDKs [89].

- Raspberry Pi: The Raspberry Pi 3 B + is a credit-card-sized computer that can connect to a monitor, a keyboard, and a mouse assembly [90]. Ultra-compact motherboard with 1.4 GHz ARM Cortex-A53 Quad-Core processor, 1 GB RAM, HDMI, 4x USB 2.0, Gigabit Ethernet, Extended 40-pin GPIO header, 5V/2.5A DC power input, and Micro SD port for storing data and loading the operating system, we have installed Raspbian Stretch as an operating system. The strong point of this new version of Raspberry Pi 3 is at the level of network connectivity. The Cypress network chip of the B + model combines Bluetooth 4.2 and Wi-Fi Dual-Band b / g / n / ac for more speed and less latency.
- ADS1115: is a 4-channel analog-to-digital converter, low-power, 16-bit. The Raspberry Pi is a digital-only computer; in other words, it cannot read analog inputs and does not include a hardware analog-to-digital converter. For this purpose, we have connected the ADS1115 between the Raspberry 3 Pi B+ and sensor to convert the out signal of the sensor (analog signal) to a digital signal with high accuracy, as shown in Figure 2.2.
- Pulse Sensor is a heart rate sensor integrated with an amplifier and noise cancellation circuit. It is based on the principle of photoplethysmography to detect volumetric variations of blood in peripheral circulation at the surface of the skin; by measuring small differences in the intensity of light transmitted through or reflected from the tissue. These variations in intensity are associated with changes in blood flow through the tissue [91]. The sensor can clip onto a fingertip or earlobe for measuring heartbeat

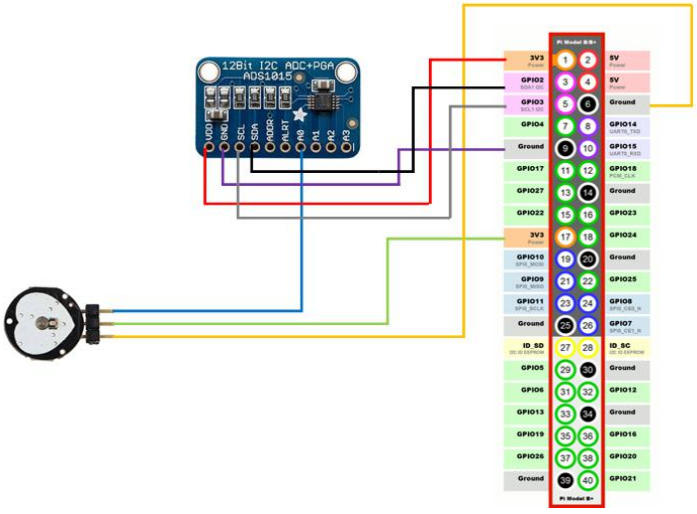

Figure 2.2. The wiring diagram of heart rate measurement device.

2.4.2 Case Study

Nowadays, around the world, there are many people whose health could be impaired by a lack of adequate health care monitoring, such as elderly patients with heart disease, where cardiovascular diseases are the world's leading cause of death, 17.9 million deaths per year have been recorded [86]. Besides, patients with coronavirus disease, that needs daily examination in quarantine. More to the point, the shortage of healthcare workers compared to the global population, according to figures from the World Health Organisation (WHO), more than 40 % of WHO Member States report having less than 10 physicians per 10 000 population and more than 26 % report having fewer than 3 [87]. The increase in the elderly population, the prevalence of chronic diseases, and the spread of coronavirus disease have further exacerbated the situation.

Urgently, healthcare needs to be transformed from a hospital-centered structure to a person-centered environment with a focus on patient wellbeing. Recent advances in IoT technologies can improve healthcare systems. Also, the possibility of a remote monitoring device will help the caregivers to have pre-diagnosis of the patient's condition and early detection before the diseases develop into a crisis stage. For these purposes, we developed a Cloud-IoT based system for patient heart rate monitoring. Healthy people can also benefit from the proposed system to check their health and wellness. The proposed system consists of four units, as shown in Figure 2.3.

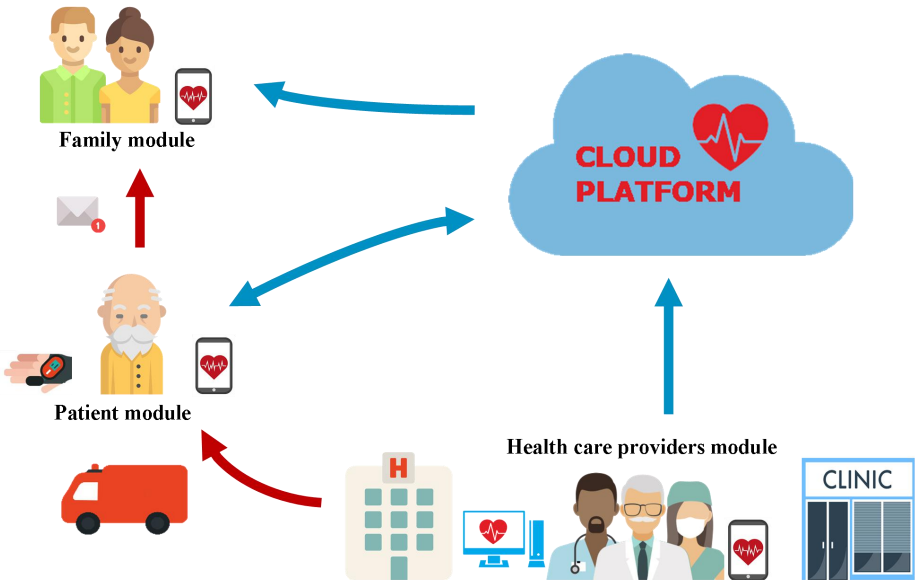

Figure 2.3. A Cloud-IoT based system for patient heart rate monitoring.

- Patient unit: consists of a wearable device prototype showing in Figure 2.4 and a mobile application. The device is responsible for sensing the patient heart rate and automatically upload the sensing data to the cloud. The patient can easily measure and monitor his heart rate anytime, anywhere. He needs to open the mobile application, log in to his account, put his finger on the heart rate sensor, and stay still. The device takes less than five milliseconds to get an accurate heart rate measurement.

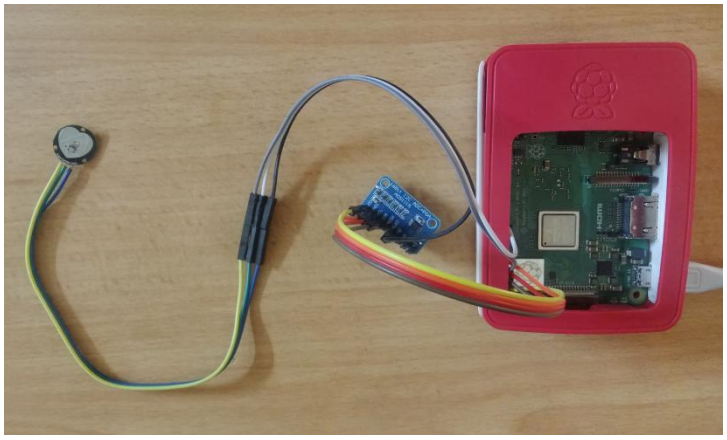

Figure 2.4. The heart rate measurement device of the proposed system.

- Family unit: consists of a mobile application that supports multiple user profiles, allowing each of the patient family members to have profiles to have their own individual measurement, and easily monitor the heart rate of family members remotely anytime, anywhere with a single app.

- Health providers unit: consists of a mobile application that allows the medical staff to easily monitor patient heart rate remotely anytime, anywhere with a single app and in real-time, see the patient medical record. Thus they can know the factors leading to the patient's deterioration, get accurate disease diagnosis, take preventive actions accordingly, identify the emergency condition for risky patients, and prepare for an immediate medical response (suggest medicines, sent the ambulance, etc.)

- Cloud unit: Cloud stores the data inside the collection (myhealthapp), each patients' medical record has its own document (user ID number). As shown in Figure 2.5, the document contains key-value (birthyear, cityCountry, code, etc.). The cloud provides patients to upload, store, and retrieve their medical data. Further, it allows health

providers and patients' family members to have ubiquitous access to patients' medical records away from hospitals and health clinics through their smartphones.

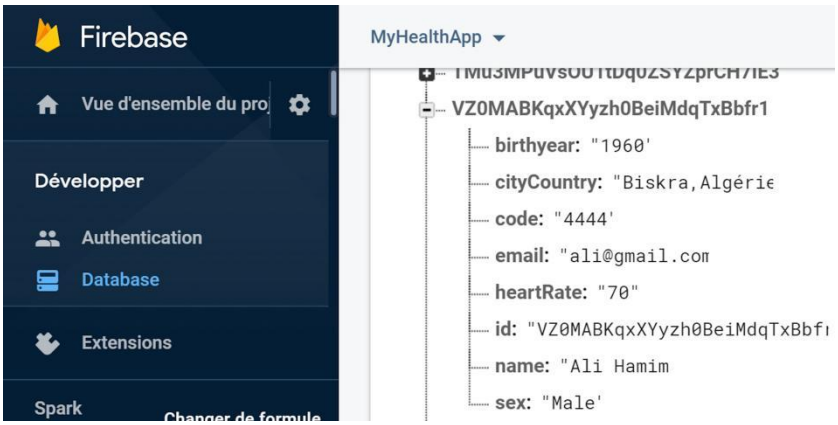

Figure 2.5. Cloud data structure of the proposed system.

2.4.3 System Interfaces

To benefit from the proposed system, we have developed a mobile phone application that provides users with various features. The mobile application interfaces are presented below. As shown in Figure 2.6, the first interface is the login interface, which enables the user to log in by using his username and password.

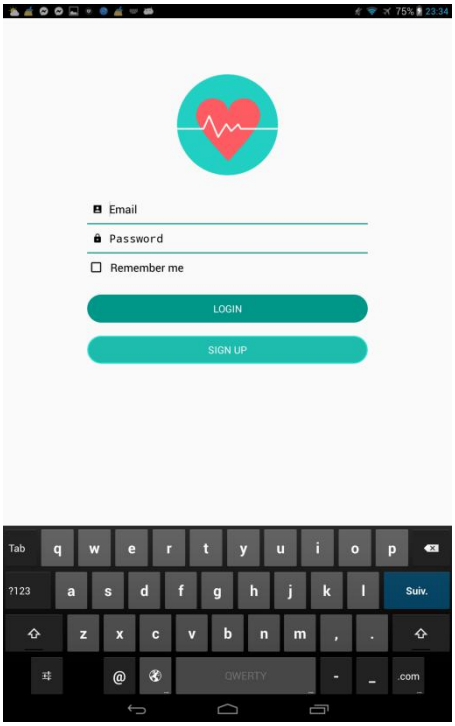

Figure 2.6. The login interface of the mobile application.

For security and control of the user information, only the registered users are allowed to use our system; thus, login requires signup. In order to create a new account, the user must insert his personal information, password, and code (the measurement device identifier) into the second interface, as shown in Figure 2.7.

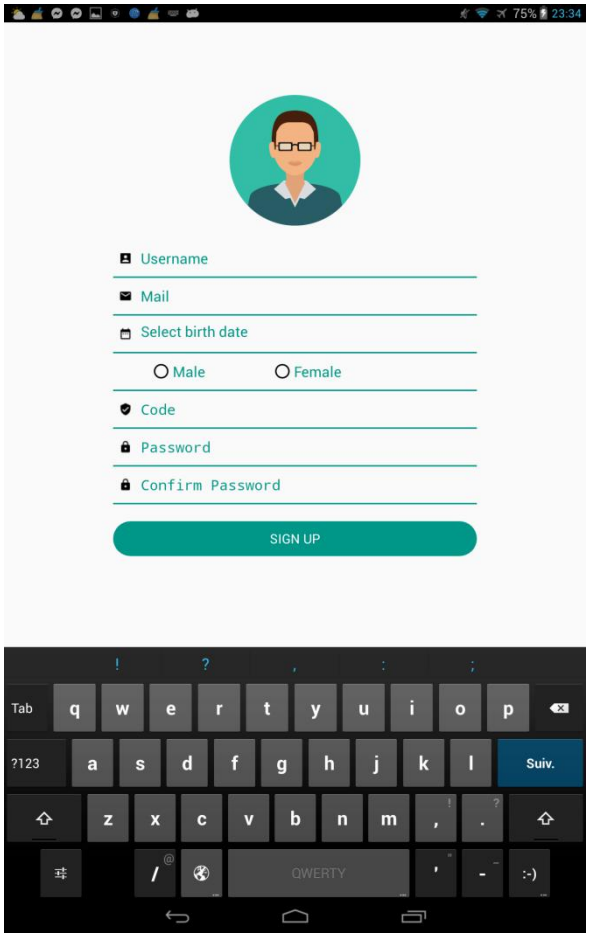

Figure 2.7. The signup interface of the mobile application.

As shown in Figure 2.8, the patient interface shows a selected portion of the patient's personal information, current location, and real-time heart rate for allowing patients, their family members, and health providers to keep track of important health information.

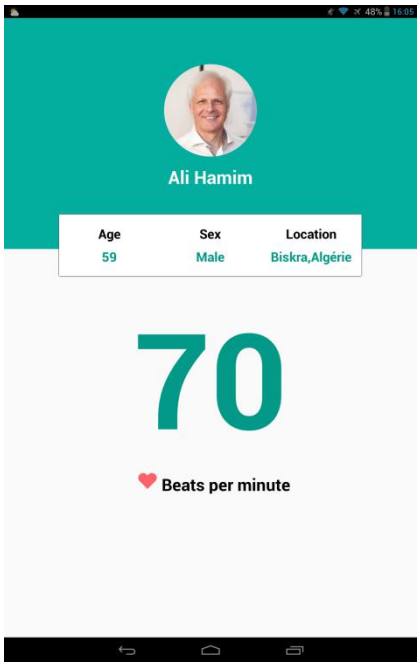

Figure 2.8. The patient profile interface of the mobile application.

The patient list interface supplies healthcare providers with easy access to patient health information, remote and real-time heart rate tracking, as shown in Figure 2.9. Also, it helps healthcare providers to understand the patient's health situations and needs. The healthcare providers can click on the patient item in the list, then get more information in the patient profile interface.

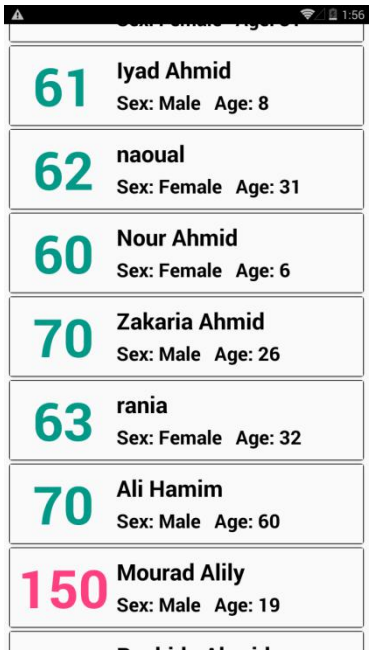

Figure 2.9. The patient list interface of the mobile application.

2.4.4 Results and Discussion

The effectiveness of the proposed system was validated by experiments in remote heart rate monitoring. For a group of volunteers contain 20 people between the age of 5 and 75 years. As shown in Figure 2.10, all user data was stored in the cloud, where each user's data was stored in a separate document.

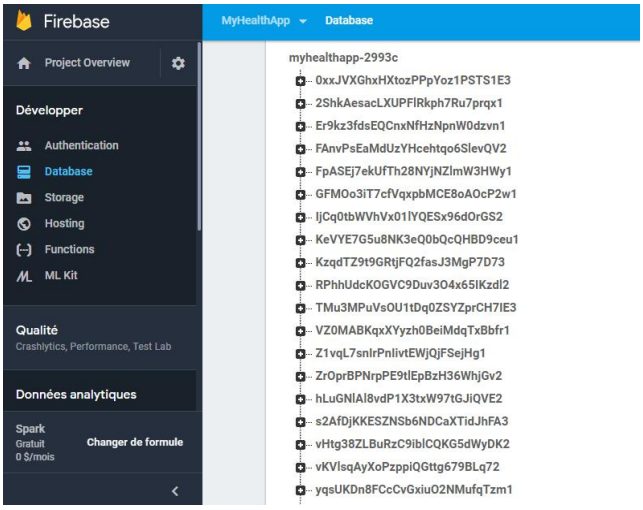

Figure 2.10. Cloud data of the proposed system.

In order to ensure the accuracy of the readings of our device, we have compared the heart rate reading of our device and the smartwatch Huawei gt 2, as shown in Figure 2.11.

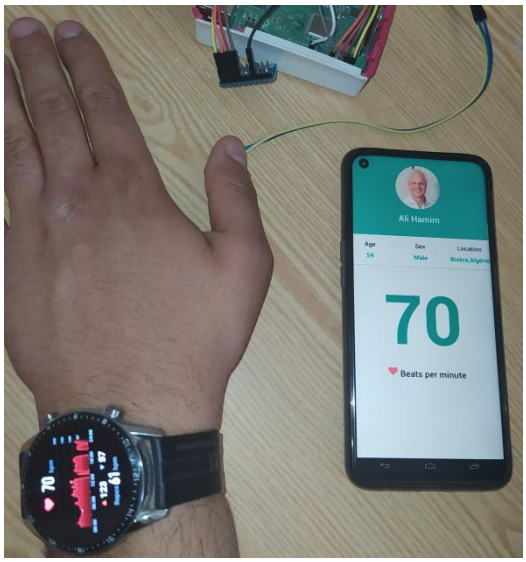

Figure 2.11. The heart rate readings of devices.

The results show that there is a good match between the two devices' readings. As shown in Figure 2.12, the mean difference between them was (± 2) beats per minute (bpm). This difference is due to the different pressure of the index finger on the sensor.

Figure 2.12. Comparison of heart rate readings between devices.

As the proposed system has the ability to monitor the patient's heart rate in the environment where the patient was located and allows healthcare providers to stay informed 24/7 through the mobile application. It would be very important for healthcare providers to understand and consider the differences that will impact the health status of these patients. The measured parameter has been shown in digital form in the smartphone application, making it easy for all users to understand in emergency and normal situations. Since it can move the treatment process away from healthcare buildings and provide patients with remote access to care services and support in emergency situations. It will reduce the regulatory burden on healthcare buildings and solve the lack of beds problem.

2.5 Conclusion

In this chapter, a Cloud-IoT approach to improve IoT scalability is proposed. In order to prove the feasibility of our approach, a Cloud-IoT system for remote heart rate monitoring is developed. The effectiveness of the proposed system was validated by experiments in remote heart rate monitoring with a voluntary group of 20 participants between the ages of 5 and 75. The experimentation showed a good match between the heart rate reading of our device and the smartwatch Huawei gt 2. The method is an effective way to improve healthcare services since it can move the treatment process

away from healthcare buildings, thus will reduce the regulatory burden on healthcare buildings and solve the lack of beds problem. Also, it can help healthcare providers to understand and consider the differences that impact the health status of patients in everyday life. On the basis of the promising findings presented in this chapter, work on the remaining issues is continuing and will be presented in the next chapters.

“Despite continued security problems, the IoT will spread and people will become increasingly dependent on it. The cost of breaches will be viewed like the toll taken by car crashes, which have not persuaded very many people not to drive.”

Richard Adler

Chapter 3

An Integrated Privacy Protection System for IoT

3.1 Introduction

IoT involves connecting a big number of smart devices and sensors embedded in everyday objects which represent things. These things are often used to sense, collect and transmit data through insecure public networks, making data more vulnerable to security and privacy concerns. Also, IoT device's limits in terms of computing, memory, and energy capacities make the adoption of the traditional methods for data protection extremely difficult and can affect the system performance parameters such as speed, size, and power consumption [92], especially in systems with strict time constraints such as real-time monitoring system, where a few seconds of delay can lead to dangerous consequences. Also, the exponential growth of connected devices and data volume aggravates security problems further [93].

IoT-based healthcare systems deal with human beings' data collected from wearable sensors, the wireless communications nature of these devices makes data more vulnerable to security and privacy concerns [94]. Medical data stored may also be accessed or stolen illegally. Which has a direct impact on the patient's privacy. Identity management, access control, and data confidentiality are three key challenges in IoT security [95]. In view of all the above problems, the purpose of this chapter is to propose an integrated privacy protection system for IoT. The proposed system consists primarily of two phases. The first phase ensures data confidentiality in the perception layer by using ECC ElGamal to secure the IoT devices' communication. The second phase controls the access to the data in the cloud through three steps: identification, authentication, and authorization.

The remainder of the chapter is organized as follows: Section 3.2 presents and discusses the related works. Section 3.3 presents the details of the proposed security system. Section 3.4 presents the experimental results. Section 3.5 concludes this chapter.

3.2 Related Works

Currently, IoT applications permeate all fields, directly affect our lives, and collect a huge amount of sensitive data that is distributed across unsecured networks, which increases the importance of data confidentiality, authentication, and access control within the IoT system. However, IoT device limits in terms of storage, computation, communication, and power make it more vulnerable to attacks. Moreover, it is hard to implement traditional security methods in IoT systems, especially in the real-time monitoring system, where a few seconds of delay can lead to dangerous consequences.

Over the years, researchers have proposed several security methods based on encryption for embedded devices to preserve information security and protect it against unauthorized access. Several authors [96-100] have proposed security models based on symmetric encryption, where the same key is used for both encryption and decryption of messages. In [96], the authors have proposed an improved preserving communication protocol for the smart home systems. The proposed protocol is based on a symmetric encryption scheme and Message Authentication Codes (MAC) to guarantee data security, integrity, and authenticity. The authors of [97] have developed a security model to secure the healthcare systems. The proposed system is based on symmetric cryptography using a hash function with a key management system. In another work [98], the authors have developed an encryption algorithm improved from Data Encryption Standard (DES) for the healthcare system's privacy protection. In [99], the authors have proposed a secure IoT-based healthcare system using BSN, which they named BSN-Care. The proposed system is based on Offset codebook mode (OCB mode) for data security. The authors of [100] have used the Advanced Encryption Standard (AES) to secure IoT camera's captured images before sending them to the cloud.

Very few publications used homomorphic encryption in the internet of things, which allows doing operations on encrypted data without decrypting it first and get the

result on the encrypted form. One of them is presented in [101]; the authors have developed an IoT data security system which they named Talos. The proposed system is based on partially homomorphic encryption. In [102], the authors have proposed a data-sharing framework for the smart grid. The proposed system is based on homomorphic encryption to protect consumer privacy in the analysis of electricity consumption reports.

In contrast, several research works [103-107] have been based on asymmetric encryption in the internet of things. Asymmetric encryption uses pairs of keys, the public key for information encryption and private key for information decryption. In [103], the authors proposed a monitoring system that collects health data from sensors, then transmitted it from gateways to back-end infrastructure. The proposed framework used public-key encryption (PKI) to secure data transmission. The authors of [104] have proposed a novel delegation-based mechanism, namely OEABE for Outsourcing mechanism for the Encryption of Ciphertext-Policy Attribute-based Encryption (CP-ABE), by delegating the most costly computations to a semi-trusted party in the CP-ABE encryption process. In [105], the authors have developed a new version of Rivest-Shamir-Adleman (RSA) to secure the information exchange between IoT devices, named the Memory Efficient Multi Key (MEMK) generation scheme. In another work [106], the authors have implemented the RSA algorithm to ensure network layer security in the smart city. In a recent paper [107], the authors have proposed a secure outsourcing scheme for RSA decryption in IoT based on the Chinese remainder theorem (CRT) to concurrently conceal the private keys and the plaintext.

The two key limitations of [96-100] research are that security keys would be lost if the key sharing is insecure. Thus, both sides of the communications get compromised, and all the encrypted data can be easily decrypted. It requires a protected channel for secret key exchange before starting data transportation through an unsecured channel. This approach may not be practical in IoT because if exists a secure channel to share the key, so no need to be using encryption in the first place. Additionally, it necessitates a large number of keys; each pair of participants wishing to share encrypted messages needs a new key, which makes the security and management of the key very challenging.

The problem with the [101, 102] approaches is that it is the ciphertexts are much bigger than the plaintexts. So the processing of these big ciphertexts is usually slower and

computationally expensive than the computation of the plaintext itself, thus making it impractical for most IoT applications. The major drawbacks of the [103-107] approaches are relatively complicated and computationally intensive, which takes more time and requires more computation resources. Asymmetric cryptography may not be practical in IoT devices with limited processing and storage capabilities.

Although all studies have studied data confidentiality, little attention has been given to real-time encryption. The speed of the cryptography algorithm is very important for monitoring systems. Since it directly affects the performance of the system. Especially in systems with strict time constraints, such as real-time monitoring systems, where a few seconds of delay can lead to dangerous consequences. Also, all the previous studies do not take into account users' authentication and authorization. Access control in data security is crucial to reduce the chance of data theft and ensure data privacy. Access controls managing user access privileges, authenticate and authorize users to access the data they are allowed to see and use based on their position in the system, and keeps unauthorized users from accessing sensitive information.

For these reasons, the present chapter proposes an integrated privacy protection system for IoT to provide a security solution at the same security level as traditional cryptography. The present work based on Lightweight Cryptography that can work over IoT devices constrained devices due to the limitation of their resources. For more data security, we have implemented an access control system to ensure data privacy. Table 3.1 summarizes the differences between our work and the previous security solutions implemented in the Internet of things, from the aspect of the encryption algorithms name and type, the key security features, and system performance.

Table 3.1. Comparison of security solutions in IoT systems.

Ref	Date	Encryption algorithms	Type	Confidentiality	Access control	Real-time
[96]	2017	AES	Symmetric cryptography	Yes	No	/
[97]	2014	/	Symmetric cryptography	Yes	No	No
[98]	2015	Improved DES	Symmetric cryptography	Yes	No	Yes
[99]	2015	OCB	Symmetric cryptography	Yes	No	/
[100]	2016	AES	Symmetric cryptography	Yes	No	/
[101]	2015	/	Homomorphic encryption	Yes	No	No
[102]	2016	/	Homomorphic encryption	Yes	No	No
[103]	2012	/	Asymmetric cryptography	Yes	No	No
[104]	2018	CP-ABE	Asymmetric encryption	Yes	No	/
[105]	2017	MEMK	Asymmetric encryption	Yes	No	/
[106]	2019	RSA	Asymmetric encryption	Yes	No	No
[107]	2020	RSA	Asymmetric encryption	Yes	No	No

3.3 Security System

Currently, IoT security is a big point of discussion; one of the key issues in IoT security is data confidentiality. However, IoT devices are unable to accommodate conventional cryptography algorithms due to IoT devices' limits in terms of storage, computation, communication, and power. In addition to that, the majority of IoT devices use wireless technologies in communication, which makes them more vulnerable to attacks such as disturbing waves and ultimately leads to steal sensitive data. Another issue facing IoT is information access control. With the increasing number of Internet of Things users and the amount of confidential data, this issue gets more complicated. The users' identity must be verified, and the access level granted to each user must be determined. The data access control refers to the authentication and authorization to prevent unauthorized users from accessing sensitive information. For these reasons, we proposed an integrated privacy protection system for IoT. The proposed system consists primarily of two phases:

3.3.1 Data Confidentiality

Data confidentiality is critical in IoT systems, where it has become a major concern for IoT users. The best way to ensure data confidentiality is cryptographic algorithms; they are commonly used to encrypt data in order to allow devices to communicate safely even over an unsafe medium. Even if the transmitting medium has been hacked, the encrypted information is virtually worthless to unauthorized individuals without the correct decryption keys. Thus, the hacker would not be able to reach the contents. However, it is not easy to enforce adequate cryptographic functions on IoT devices due to their limited capabilities. In contrast to conventional cryptographic algorithms, the Curves Cryptosystem ElGamal algorithm (ECC ElGamal) has very small keys at the same security level. These advantages make ECC ElGamal more suitable to be used in IoT devices' communication security. For those reasons, we have adopted ECC ElGamal to secure the IoT devices' communication.

For system initialization, let an elliptic curve group *Ep (a,b)*, using the elliptic curve over a finite field (p) where P is a large prime, α is a primitive root of P as

described in Algorithm 1, such that satisfy the equation (3.1) for $0 < x < P$, a and b determine the curve shape and satisfy the equation (3.2) P and α are public numbers.

$$y^2 = x^3 + a\,x + b \tag{3.1}$$

$$4\,a^3 + 27\,b^2 \neq 0 \tag{3.2}$$

Algorithm 1 Initialization

```
1 :   P = large prime ();
2 :   α = Base ();                    // Base point
3 :   ECC_2_Equation (a, b);          // (3.2)
End
```

In order to establish secure communications between device and gateway (D, G), device as a sender and gateway as a reserve, D creates a key pair $\{d, \beta_d\}$ as (3.3) where d is the private key and β_d is the public key of D device as described in Algorithm 2. The same thing for G (3.4).

$$\beta_d = d\,\alpha \tag{3.3}$$

$$\beta_g = g\,\alpha \tag{3.4}$$

Algorithm 2 Key Generation of device

```
1 :   d = random () ;          // private key
2 :   βd = d * α ;             // public key
3 :   k = random () ;          // secret number
End
```

When the device wants to send the information i to the gateway, the device converts the information i to a point I on the elliptic curve E by using a mapping function *map()*. Also, choose a random integer k, and keep it secret, calculate the pair point $\{Y_1, Y_2\}$. Then, mapping the pair point $\{Y_1, Y_2\}$ into the pair point $\{Y_{1m}, Y_{2m}\}$ by using the mapping function *map()* and sends them to the gateway as shown in Figure 3.1.

$$Y_1 = k\,\alpha \tag{3.5}$$

$$Y_2 = I + k\,\beta_g \tag{3.6}$$

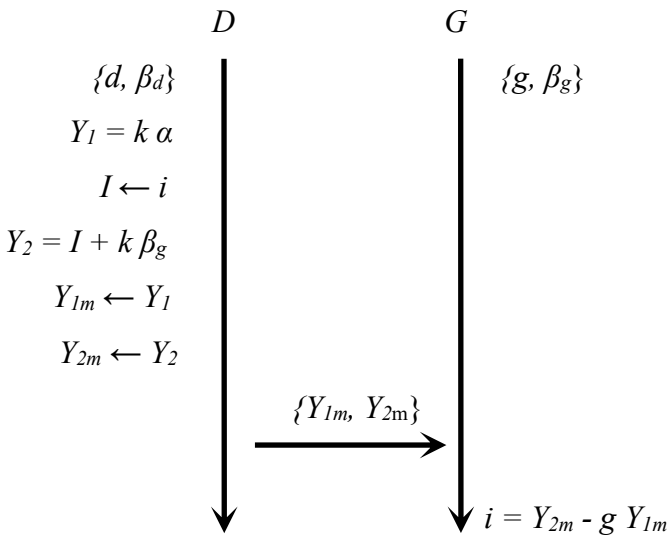

Figure 3.1. Interaction diagram of the ECC ElGamal cryptosystem.

ECC ElGamal algorithm can only encrypt and decrypt a point on the curve, not the information. Based on that we have encrypted the information characters one by one by mapping the character to a point on the curve where each character of the information represents a point in ECC ElGamal. Then encrypt it and map it again to another point as illustrated in Algorithm 3.

Algorithm 3 Encryption

Input: bytes[] and point β_g

Output: Pair of point Y_1, Y_2

```
1:    var s : integer;  s = size (bytes []);
2:    var result : array [s * 2] of byte;
3:    var p : array [s] of point;
4:    var j, i : integer;  j = 0;
5:    For  i = 0 to s do
6:        p [i] = map (bytes [i]);
7:        Y1 =  k * α;          Y2 = p [i] + (k *  βg);     // encryption of point p [i]
8:        result [j] = map (Y1);
9:        j = j + 1;
10:       result [j] = map (Y2);
11:       j = j + 1;
12:   End
```

```
13:     Return result;
14:End
```

When the gateway receives the ciphertext, it uses his private key g to decrypt the information I point by point, then recovers the readable information as shown in algorithm 4.

$$i = Y_2 - g\ Y_1 \tag{3.7}$$

Algorithm 4 Decryption

```
Input: bytes[]  and g;
Output: result array [] of byte;
1:      var s : integer;  s = size(bytes []);
2:      var result : array [s / 2] of byte;
3:      var j, i : integer;  j = 0;
4:      For  i = 0 to size (result []) do
5:           j = j + 2;
6:          // Decryption by point
7:          result [i] = bytes [j + 1] - (bytes [j] * g )
8:      End
9:      Return result;
10:End
```

3.3.2 Access Control

Access control on IoT cloud systems is crucial to ensure the privacy of health information and personally identifiable information of users, also limiting information access to only authorized people. The access control systems can avoid unauthorized access in the cloud data, reduce chances of the privacy breach and data leaks occurring. To provide a high-security level, we have developed an access control system that can authenticate and authorize users to access the health data they are allowed to see and use according to their roles. As shown in algorithm 4, the proposed system has three steps: identification, authentication, and authorization.

First, we verify the users' identities that request access to a system. The user must have an identity in the system so that the authentication method can interrogate the account. The authentication process has two steps and if one of these steps fails, the access will be denied. First, the mobile application will prompt the user to enter a username and password that will be submitted to the cloud server to check whether the username is already in the users' list. Once the provided password matches the user's password stored in the cloud, the authorization process begins.

In the authorization process, the system will verify whether or not the user is authorized to access data through verifying the access permissions for this user that determined by the metadata concerning the user's account. Once a user is given the authorization to access a specific part of data on the cloud, he can perform a set of actions according to his role. The proposed system has different levels of access control, healthcare providers have access to all patient information, the patient can monitor his heart rate, and it can also monitor their family members' heart rate if they invited him.

Algorithm 5 Access Control

Input: identification, password, and query;

Output: query result;

1: The user provides a username (UN) and password (PW) to the mobile applicatio;
2: The mobile application will pass the UN and PW to cloud servers;
3: Cloud servers research the username;
4: **If** exists and PW matches the user's password stored do
5: **If** the user is a healthcare provider do
6: Show all health information of patients;
7: **Else**
8: Show only the health information of the user
Show list of family members who invited him
9: **Else**
10: Denied the access and shows an error message
11: **Return** query result;
12:**End**

3.4 Experimental Evaluations

In this section, we demonstrate the efficiency of our system by comparing it to other systems in terms of computational and storage costs. The experimental results are presented in charts.

3.4.1 Experimental Setup

For experimental evaluation, we have implemented the proposed system in raspberry pi 3 B +, with 1 GB RAM, 1.4 GHz ARM Cortex-A53 Quad-Core processor, micro SD 32 GB, and Raspbian Stretch as an operating system. In order to test the performance of our ECC ElGamal implementation, we also implemented public key algorithms ElGamal and RSA, with keys' long based on the recommendation of the National Institute of Standards and Technology (NIST) [108], and we measured the encryption and decryption time of the same message with 160 bits long on three different security levels.

3.4.2 Results and Discussion

The bar chart compares the key size between the three algorithms RSA, ElGamal, and our implementation of ECC ElGamal in three security levels. Overall, both asymmetric algorithms RSA and ElGamal have long key size, while ECC ElGamal key size is shorter than other algorithms in all security levels as shown in Figure 3.2. RSA and ElGamal key size was 1024 bits long in the first security level, being longer than ECC ElGamal's key size by approximately 864 bits. Then, it rose to 2048 bits in the second security level and continued to increase steadily to 3072 bits in the last security level. However, ECC ElGamal's key size was 160 bits in the first security level. The bar chart showed a gradual increase to 224 bits in the second security level and continued to increase steadily to 256 bits, being shorter than other algorithms' key size by approximately 2816 bits in the last security level.

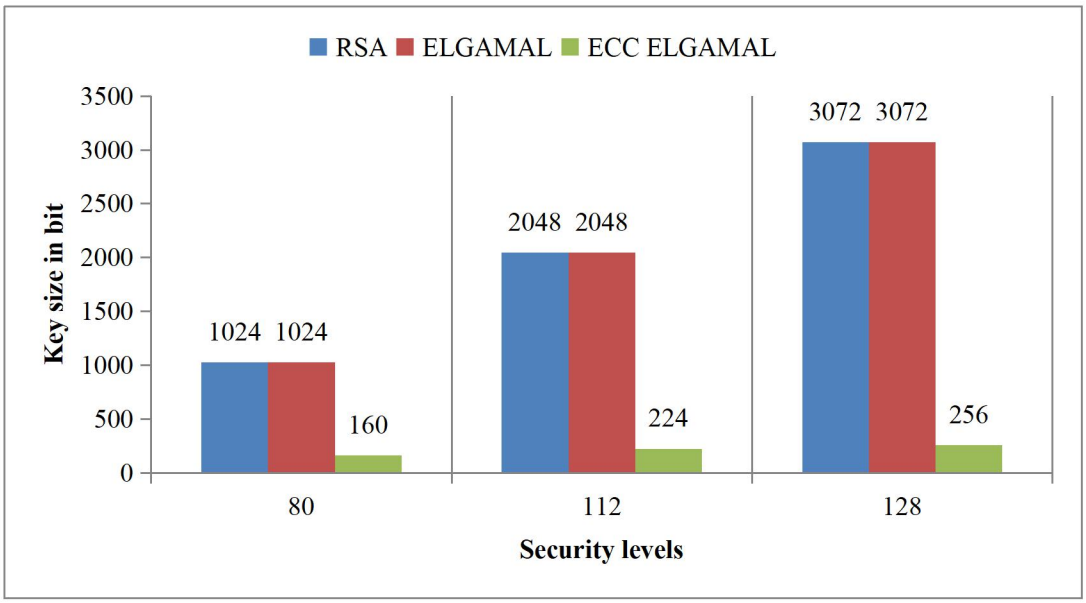

Figure 3.2. Comparative analysis of algorithms' key size.

As shown in Figure 3.3, the bar chart shows the encryption time taken to encrypt the same message by the three algorithms in three different security levels. Overall, both asymmetric algorithms RSA and ElGamal take longer, while ECC ElGamal takes much less time than other algorithms in all security levels. In the first security level, the encryption time taken by the RSA and ElGamal was 0,231 seconds and 0,145 seconds respectively. Then, RSA and ElGamal's encryption time continued to increase sharply throughout the security levels. Where RSA rose significantly to 4,78 seconds, being longer than ElGamal's encryption time by approximately 1,833 seconds in the last security level. However, ECC ElGamal's encryption time was 0,011 seconds in the first security level. Then, it gradually increased to 0,017 seconds in the last security level, being shorter than RSA and ElGamal's encryption time by approximately 4,77 seconds and 2,93 seconds respectively.

The bar chart illustrates the decryption time taken to decrypt the same message by RSA, ElGamal, and our implementation of ECC ElGamal algorithms in three different security levels, as shown in Figure 3.4. Units are measured in seconds. Overall, the decryption time of RSA and ElGamal algorithms was higher than that of ECC ElGamal. In the first security level, the decryption time taken by the RSA and ElGamal algorithms was 0,483 seconds and 0,203 seconds respectively. Then, RSA and ElGamal's decryption

time continued to increase sharply throughout the security levels. Where RSA rose significantly to 7,626 seconds, being longer than ElGamal's decryption time by approximately 2,467 seconds, in the last security level. However, ECC ElGamal's decryption time was 0,003 seconds in the first security level. Then, it gradually increased to 0,006 seconds in the last security level, being shorter than RSA and ElGamal's decryption time by approximately 7,620 seconds and 7,153 seconds respectively.

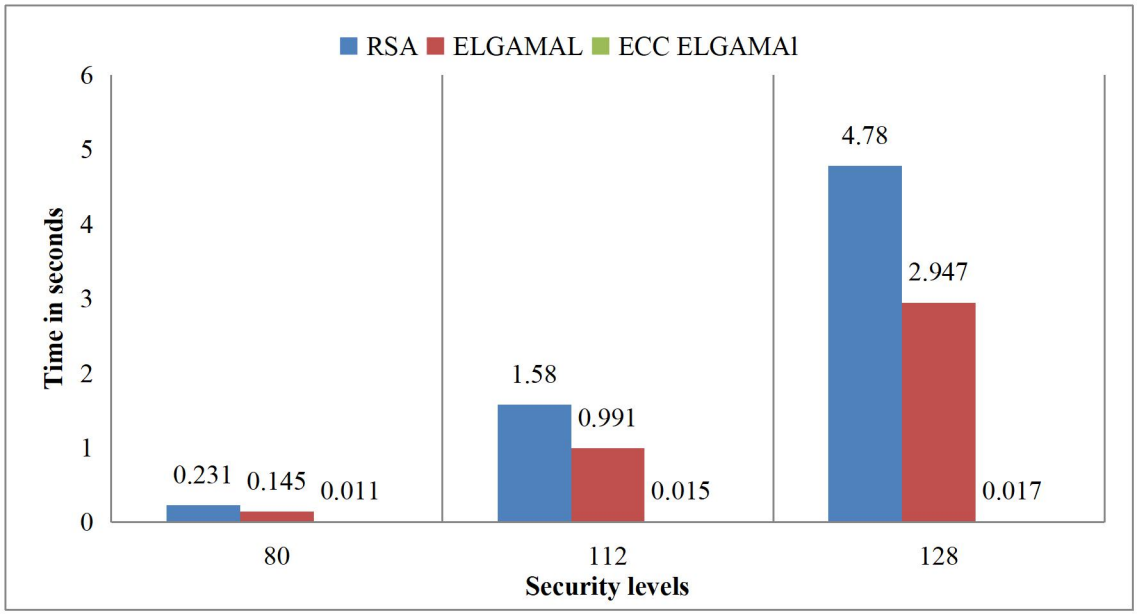

Figure 3.3. Comparative analysis of algorithms' encryption time.

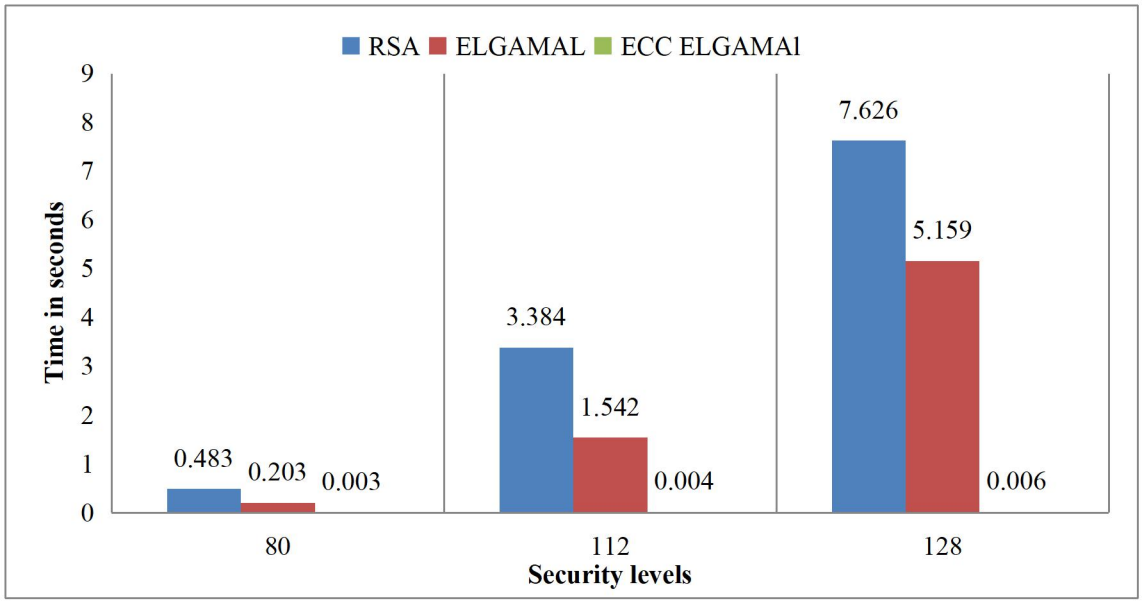

Figure 3.4. Comparative analysis of algorithms' decryption time.

In contrast to RSA and ElGamal algorithms, ECC ElGamal offers high security using less computing power, and memory, resulting in much faster response times and better performance. This benefit would be very important for IoT devices with limited processing power, memory, and energy capabilities. ECC ElGamal can be the next-generation implementation of public key cryptography, and the best alternative for IoT devices.

3.5 Conclusion

In this chapter, an integrated privacy protection system for IoT is proposed. In order to ensure the user's data privacy, we have encrypted the data by ECC ElGamal to secure the IoT devices' communication in the perception layer. We have also developed an access control system for the data in the cloud. In order to verify the efficiency of the proposed system, we have compared our implementation of ECC ElGamal with other systems in terms of computational and storage costs in three different security levels. The experimentation shows that ECC ElGamal was more suitable to be used in IoT devices' communication security, where ECC ElGamal takes much less time than other algorithms in all security levels.

“Without intelligence there is no value.”

Kiva Allgood

Chapter 4

A Cloud-IoT System Based on Smart Agent

4.1 Introduction

Currently, one of the most key problems that facing IoT is heterogeneous device management. While the loT system shows capable of making decisions and interacting intelligently with its devices, the real situation is that these devices are still not smart enough to make quick and smart decisions in dangerous situations [109], [110]. It works so based on specific business rules and does not take into account unexpected environmental changes. Furthermore, the ability of devices to communicate with other devices is dependent on service similarity and contact protocols. When IoT devices can process data, make decisions, and act on that data without requiring human intervention, IoT apps can reach their full potential [111], [112]. In view of all the above problems, an integrated system that combines IoT and intelligent agent technology to enhance IoT intelligence has been proposed. Specially, we have proposed a Cloud-IoT system based on smart agents. The proposed system consists of a group of agents distributed in the four IoT architecture layers; a group of agents collaborates to collect, process, and store data in the cloud. The remaining agents are deployed on IoT devices.

The remainder of the chapter is organized as follows: Section 4.2 introduces the different definitions, classifications, and characteristics of agents, as well as the multi-agent system. Section 4.3 presents and discusses the related works. Section 4.4 presents the details of the proposed approach. Section 4.5 presents the experimental results. Section 4.6 concludes this chapter.

4.2 Background

In this section, we present a brief background of the agent and the multi-agent system technologies.

4.2.1 Definition of Agent

Although the term "agent" is commonly used, it has numerous contradictory definitions. The more detailed definition of the agent is given by Jacques Ferber where it combines the agent's functioning and its capacities [113]:

"An agent can be a physical or virtual entity that has the capacity to:

- Act in an environment,
- Communicate directly with other agents,
- Be equipped with a set of trends (in the form of individual objectives or satisfaction or even survival function, which it seeks to optimize),
- Has its own resources,
- Perceive (but in a limited way) his environment,
- Only have a partial representation of this environment (and possibly none),
- Have skills and offer services,
- To reproduce, possibly,
- Behave which tends to meet its objectives, taking into account the resources and skills at its disposal, and according to its perception, its representations, and the communications it receives."

According to Jennings, Sycara, and Wooldridge [114]: "An agent is a computer system, situated in some environment, that is capable of flexible autonomous action in order to meet its design objectives."

According to these definitions, an agent is a physical entity acts in an environment, endowed with sensors and shareholders; it decides for itself what it must do to achieve its objectives (determined at its design), considering the capabilities at its disposal.

4.2.2 Characteristics of Agent

The agent community defines a set of agent characteristics. In fact, they are frequently true, but not always the case [115].

- Autonomy: is the most interesting characteristic of the agent in which he can independently take the appropriate decision without the intervention of other agents or even human intervention. Also, execute the necessary action, and control its' own internal state [117].
- Flexibility: A flexible agent must be [116]:
  - Reactive: In this case, the agent is able to perceive the environment in which he has situated, which may be an agent container, an application, a physical device, and Internet, then react to changes in time.
  - Proactive: The agent's behavior is determined by his goals, and therefore he can produce goal-directed actions, as well as take the necessary initiative, not just responses to his environment.
  - Social: An agent must have the ability to interact with external sources (other agents, system or even humans) when he needs to ask for help, share/obtain knowledge, and negotiate in order to meet his goals.
- Situation: The agent is located in an environment; if he can perceive his environment thanks to the sensory inputs he receives from this same environment and modify his behavior accordingly at all levels (objective, plan, action, etc.) [116].
- Reasoning: An agent can deduce and create knowledge based on the information he has collected. Then, he can decide which goal to pursue, [118] which event to react to, how to act to accomplish a goal, or even suspend or abandon others [116].
- Adaptive: an agent has this property if he can use his knowledge to modify his behavior and automatically adapts to changes. Also, he can control his skills according to the agent or the environment with which he interacts [115].

4.2.3 Classification of Agent

According to Ferber Jacques, there are two main types of agents [119]. This classification is based essentially on the agent's decision-making process and the representation of the environment at his disposal.

- Cognitive agent: endowed with reasoning and planning skills and communication skills, can solve complicated problems in a relatively individual way [119], thanks to his knowledge base, which comprises all the information and knowledge necessary for carrying out his task and managing interactions with other agents and with his environment [120].
- Reactive agent: can perceive the environment and only reacts to changes in the environment [119]. In other words, such an agent does not do any deliberation, knowledge, or planning. Reactive agent decision-making based on Stimulus/Response; he simply acquires perceptions and reacts to them. Since there is no reasoning, these types of agents can act and react very quickly [121].

The combination of the two previous models of agents results in a new hybrid agent that combines reactive and cognitive abilities, allowing them to adapt their behavior in real-time to changing environments. In this model, the agent has a multi-layered architecture, each layer being either a cognitive component or a reactive component [122].

4.2.4 Definition of Multi Agent System

There are several attempts to define multi-agent systems (MAS). One of the most common definitions is proposed by Jacques Ferber [113]:

"We call a multi-agent system (or SMA), a system composed of the following elements:

- An environment *E*, i.e., space generally having a metric.
- A set of objects *O*. These objects are situated, i.e., for any object, it is possible, at a given moment, to associate a position in *E*. These objects are passive, i.e., they can be perceived, created, destroyed, and modified by agents.
- A set of agents *A*, which are particular objects (*A* includes *O*), which represent the active entities of the system.

- A set of relations *R* which unite objects (and therefore agents) between them.
- A set of operations *Op* allowing agents of *A* to perceive, produce, consume, transform and manipulate objects of *O*.
- Operators responsible for representing the application of these operations and the world's reaction to this attempted modification, which will be called the laws of the universe. "

4.2.5 Characteristics of Multi Agent System

The MASs are used efficiently in several fields, thanks to these characteristics. In the following, we listed the most important characteristics of MAS.

- Distribution: The system is decomposable, with the agent as the primary component. The system's agents may be located in different locations [123].
- Leadership: there are two types [124]:
  - Leader-following or centralized MAS: has an agent as a leader; he establishes goals and tasks for the other agents based on a single global goal.
  - Leaderless or decentralized MAS: the agents are independent, and there are no centralized decisions valid for the whole system.
- Heterogeneity: MAS can be classified into two categories based on agent heterogeneity [124]:
  - Homogeneous MAS refer to agents with similar characteristics and functionalities,
  - Heterogeneous MAS refer to agents with a variety of characteristics and functionalities.
- Topology: based on the agent's location and relations can be classified into two categories [124]:
  - Static topology: an agent's location and relationships remain the same throughout his lifetime.
  - Dynamic topology: in this topology, the agent's location and relationships change; an agent can move, exit, or join the MAS; or even forms new communications with other agents.

4.3 Related Works

Currently, IoT represents a revolutionary concept, rich in potential as well as in development problems such as decentralization, intelligence, and scalability. Very few publications have been based on the decentralized MAS. Agents in the decentralized MAS can work independently and collaborate with each other to accomplish the global goal [133]. In [125], the authors have proposed an Agent-based architecture for smart objects-oriented Cloud-IoT systems, which they named CA-IoT. The proposed framework consists of a group of agents embedded in a cyber-physical world, combined with a cloud, and interfaced with external IT systems. The authors of [132] have proposed a framework for monitoring the civil infrastructure based on agents for remote access and autonomously process collected information. In [135], the authors proposed an agent-based traffic administration system for traffic monitoring and managing.

In contrast, several research works [103-107] have been based on the centralized MAS as shown in Table 4.1, where a single agent acts as a central agent in centralized MAS, determining the system's state depending on the information available from all other agents. The central agent makes an optimal decision based on the information obtained [133]. The authors of [126] have developed an agent-based health care monitoring system. The proposed system can sense vital signs of the patient, such as body temperature, blood pressure, heart rate, and respiratory rate by using WSNs. In a recent paper [127], the authors have developed a multi-agent-based mobile healthcare system for enhancing interaction among patients, caretakers, doctors, and other healthcare providers. The authors of [128] have designed a distributed information platform based on mobile multi-agent for support the intensive and distributed nature of wide-area monitoring environment, named MADIP. MADIP is made up of two groups of agents: static agents and mobile agents.

In [129], the authors have proposed an activity monitoring system for promoting the elders' healthy lifestyles and diagnose psychomotor abnormalities early. In [130], the authors proposed a mobile gateway solution based on agents for mobile health scenarios. This gateway autonomously collects patient's information. Then it forwards the collected data to the healthcare providers. The authors of [131] have proposed an agent-based

architecture for mobile health monitoring, which includes a set of intelligent agents who gather patient data, reason together, and suggest actions to patients and medical staff. In [134], the authors develop an automatic diagnosis engine based on mobile agents to support intensive and distributed ubiquitous fetal surveillance without interruption with the normal routines of the patient and without limiting her mobility.

The major drawback of the [126-134] approaches is it based on centralized MAS. In centralized MAS, a single agent performs all the major processing, has complete control over all aspects of the system, and makes decisions based on analyses of information gathered by other agents. This approach may not be practical in all situations, it is computationally intensive, less flexible in terms of analysis and decision making. Also, it is more vulnerable to failure in case of the central agent goes down/dead for some reason and the other agents are unable to handle requests; it would most likely bring the whole IoT system down with it.

In contrast, the [125], [132], and [135] approaches are based on decentralized MAS, where each agent within the system acts as an autonomous entity with decision-making authority. Another significant benefit of decentralized MAS is efficiency; there is no single point of failure since each agent acts as an individual system. If one agent fails, the remaining agents will continue to function.

However, most of the previous studies do not take into account parallel computation. The system must be able to keep up with multiple customer demands in order to have an effective IoT system. The agent's parallel behavior allows the execution of simultaneously multiple actions, unlike serial behavior. It can reduce runtime, speeds up a system's operation, and increase operational efficiency.

For these reasons, the present chapter proposes a Cloud-IoT system based on smart agents for the health monitoring of cardiovascular patients. This approach conforms to the approaches proposed in the previous chapters. The proposed system can collect, retrieve, store, and analyze the heart rate of the patient in a secure way. It can also detect the critical case immediately and take a quick and smart decision. It can be used not only by the hospital but also by any health care provider.

Table 4.1 summarizes the differences between our work and the previous agent-based solutions implemented in the Internet of things, from the aspect of the agent behavior and MAS leadership characteristic.

Table 4.1. Comparison of agent-based solutions in IoT systems.

Ref	**Date**	**Agent Behavior**		**Leadership**
		Parallel	**Autonomy**	
[125]	2014	No	Yes	Decentralized
[132]	2012	No	Yes	Decentralized
[126]	2013	No	No	Centralized
[127]	2019	No	No	Centralized
[128]	2011	No	No	Centralized
[129]	2012	No	No	Centralized
[130]	2016	No	/	Centralized
[131]	2008	No	No	Centralized
[134]	2014	No	/	Centralized
[135]	2015	No	Yes	Decentralized

4.4 Proposed Approach

For dealing with a dynamic system like IoT, a multi agent system is good solutions, to enhance the IoT system intelligence, encapsulate the complex functionalities, underlying heterogeneous hardware, and implementation details, maximizing interoperability among heterogeneous resources, increasing scalability. For this purpose, a Cloud-IoT system based on smart agents is proposed, and we named it A-IoT. In the following, we will present the details of the proposed system.

4.4.1 System Architecture

The main idea of this approach is to enhance the IoT system's intelligence by adding a vertical layer of agent to the IoT architecture. The agent layer shown in Figure 4.1., is a set of agents distributed in the four horizontal IoT architecture layers; a group of agents collaborates to collect, process, and store data in the cloud. The remaining agents are deployed on IoT devices. The agents can directly control the hosting device and its physical elements. It can also communicate and collaborate with other agents to complete their acts and objectives. It also reacts intelligently with complex scenarios without requiring active human interaction. In the following, we will explain in detail the different agents' roles.

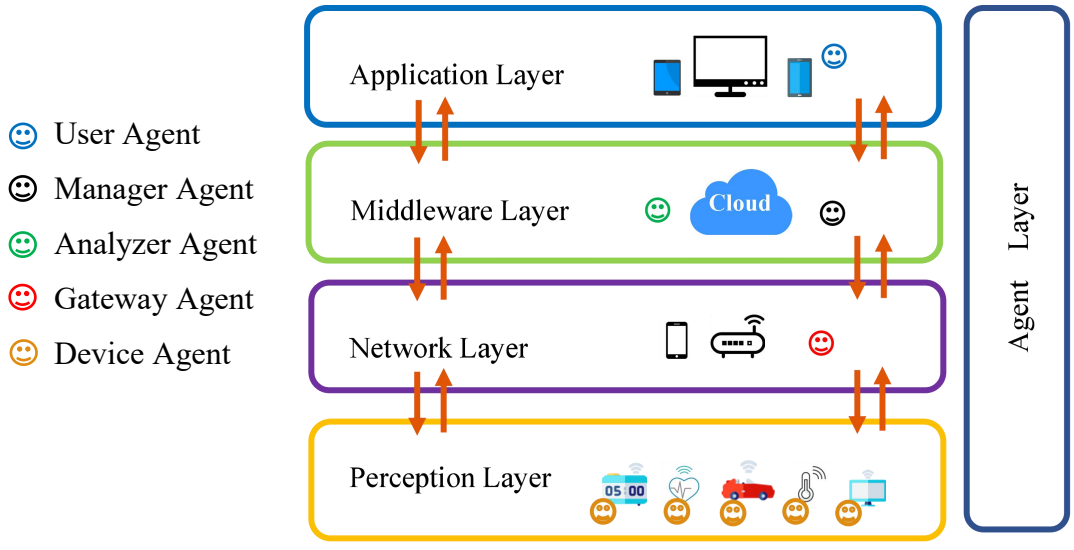

Figure 4.1. System global A-IoT architecture [136].

- Device Agent (DA): an embedded agent in each IoT device, as shown in Figure 4.2, this agent is composed of three modules: communication module with other agents, a rule base that includes all rules of this agent, and the reasoning module. Device agent responsibilities are as follows:
  - Environment perception, save the perception data, which will be encrypted before being sent to the gateway agent.
  - Control of IoT device and adjust the device state based on the user and environment needs.
  - Communicate with other agents.

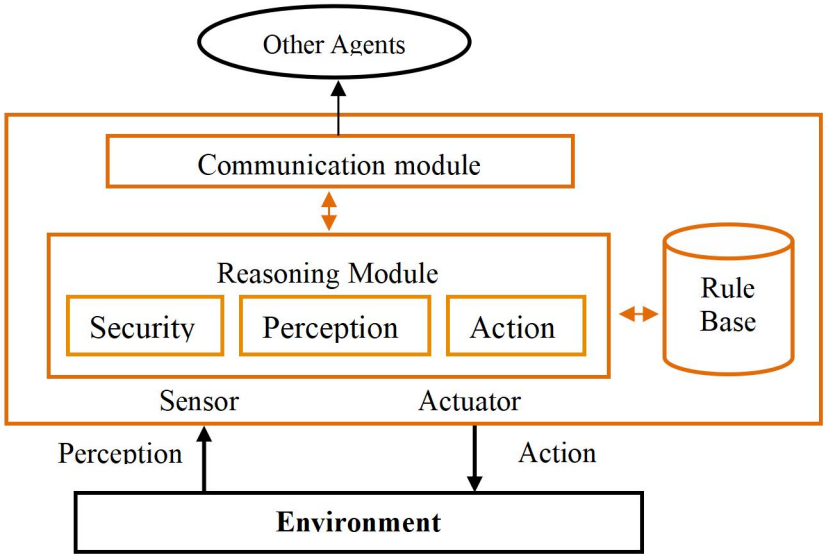

Figure 4.2. The architecture of device agent.

- Gateway Agent (GA): an embedded agent in the IoT gateway, as shown in Figure 4.3, this agent is composed of the following modules: two communication modules, the Wide Area Network (WAN) communication module to communicate with the manager agent in the cloud, and Personal Area Network (PAN) and local area network (LAN) communication module for the communication with the device agents. Security module handles data flowing in two directions from/to devices agent, in a secure way. Treatment module for the treatment of sensing data before sending it to the cloud for reducing the amount of data that must be forward to the cloud to speed up the reply times. This agent responsibilities are as follows:

- Aggregate the sensing data from device agents, decryption/encryption of the sensing data, and pre-analysis them.
- Save data for a short time in case of network failure.
- Sent the sensing data to the manager agent in the cloud.
- Communicate with other agents.

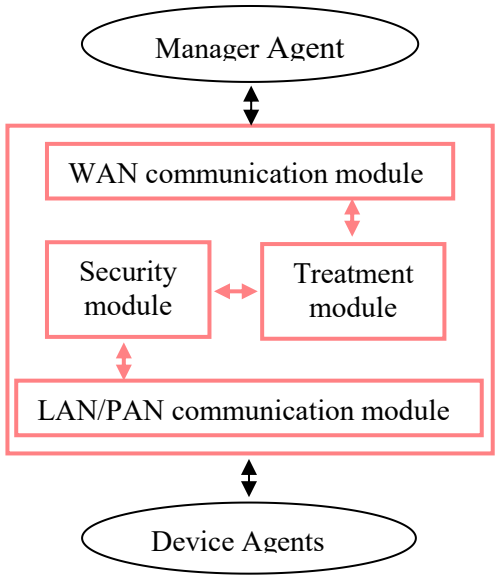

Figure 4.3. The architecture of gateway agent.

- Manager Agent (MA): an included agent in the cloud, as shown in Figure 4.4, this agent is composed of the following modules: communication module to communicate with the other agent, treatment module for the data treatment before saving it in the cloud database, management module for data management. This agent responsibilities are as follows:
  - Data collection, storing, recovery, and processing.
  - Communication with other agents.

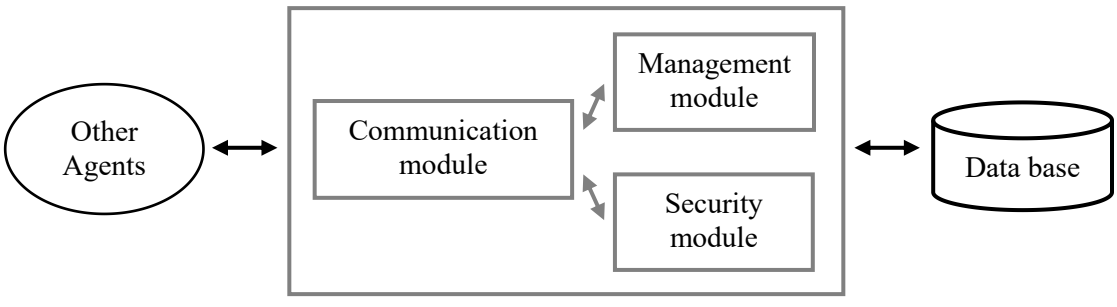

Figure 4.4. The architecture of the manager agent.

- Analyzer agent (AA): an included agent in the cloud, as shown in Figure 4.5, this agent is composed of the following modules: communication module to communicate with the other agent, analyzes module for analyzes of user's data, and security module for verification of user's privilege. This agent responsibilities are as follows:
  - User's authentication and authorization verification.
  - Analyzes the user request, then sends it to the manager agent for request execution, and returns the result to the user agent.
  - Communication with other agents.

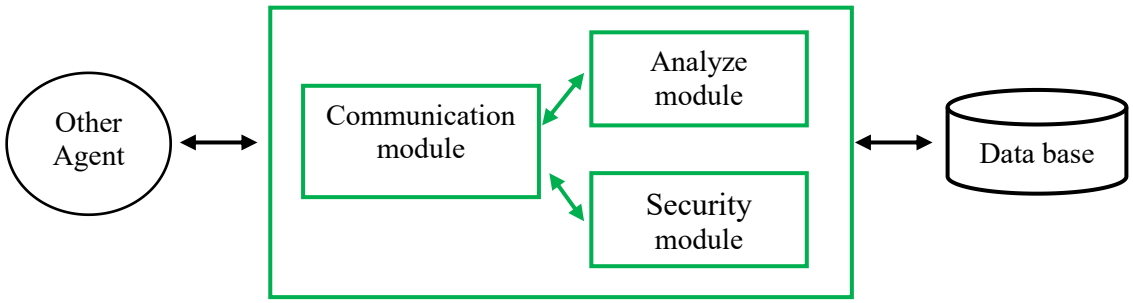

Figure 4.5. The architecture of the analyzer agent.

- User agent (UA): an embedded agent on the user device, as shown in Figure 4.6, this agent is composed of the following modules: communication module to communicate with the analyzer agent, interface module to provide a graphical interface to interact with our system and treatment module for user requests treatment. This agent responsibilities are as follows:
  - Acquire user requests.
  - Send those requests to the analyzer agent.
  - Present the results to the users.
  - Communicate with analyzer agents.

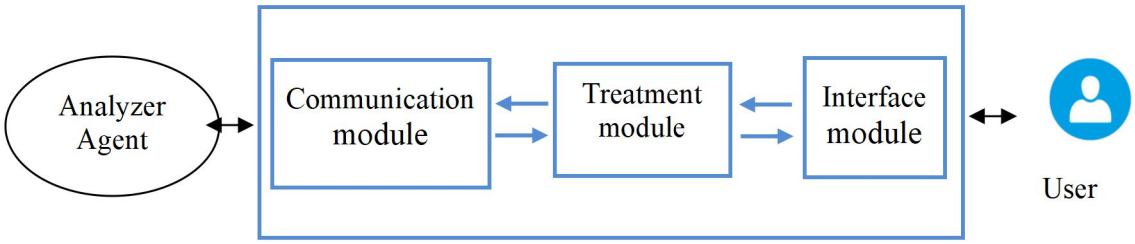

Figure 4.6. The architecture of the user agent.

4.4.2 Agents Interactions

A shown in Figure 4.7., the diagram contains three alternative that shows the different agents and their interactions in the proposed scheme, as well as the chronology of these interactions; we will explain it in depth below:

The user sends the login request to a user agent, who then sends the user login information (user Id and password) to the analyzer agent. After that, the analyzer agent returns the response to the user agent. As shown in the authentication alternative, the request will be passed only if the access information is correct, at which point the user agent will load the monitoring interface of the application; otherwise, the request will be abandoned.

After successfully signing in, if the user wants to know critical information or do an action that needs authorization, the user agent then sends the authorization request to the analyzer agent, which contains the user Id and query type. Then, the analyzer agent checks if the user is authorized or not, as shown in the authorization alternative; if the user is authorized, the analyzer agent sends the request to the manager agent; otherwise, the request will be ignored.

As shown in the request alternative, if the request type is get state, the manager agent sends a request to the gateway agent containing the device Id in order to obtain the device state. Otherwise, the manager agent sends a request to the gateway agent containing the system Id and the new state to change the device state. In all instances, the gateway agent encrypts the request before sending it to the device agent, and the device agent receives and decrypts the encrypted request. The device agent will then execute the request and transmit the device state to the gateway agent. The gateway agent receives the decrypted device state and sends it to the manager agent. The manager agent then collects, stores, processes, and passing the device state over to the analyzer agent. The analyzer agent collects the device state and transfers it to the user agent to display the result in the user application.

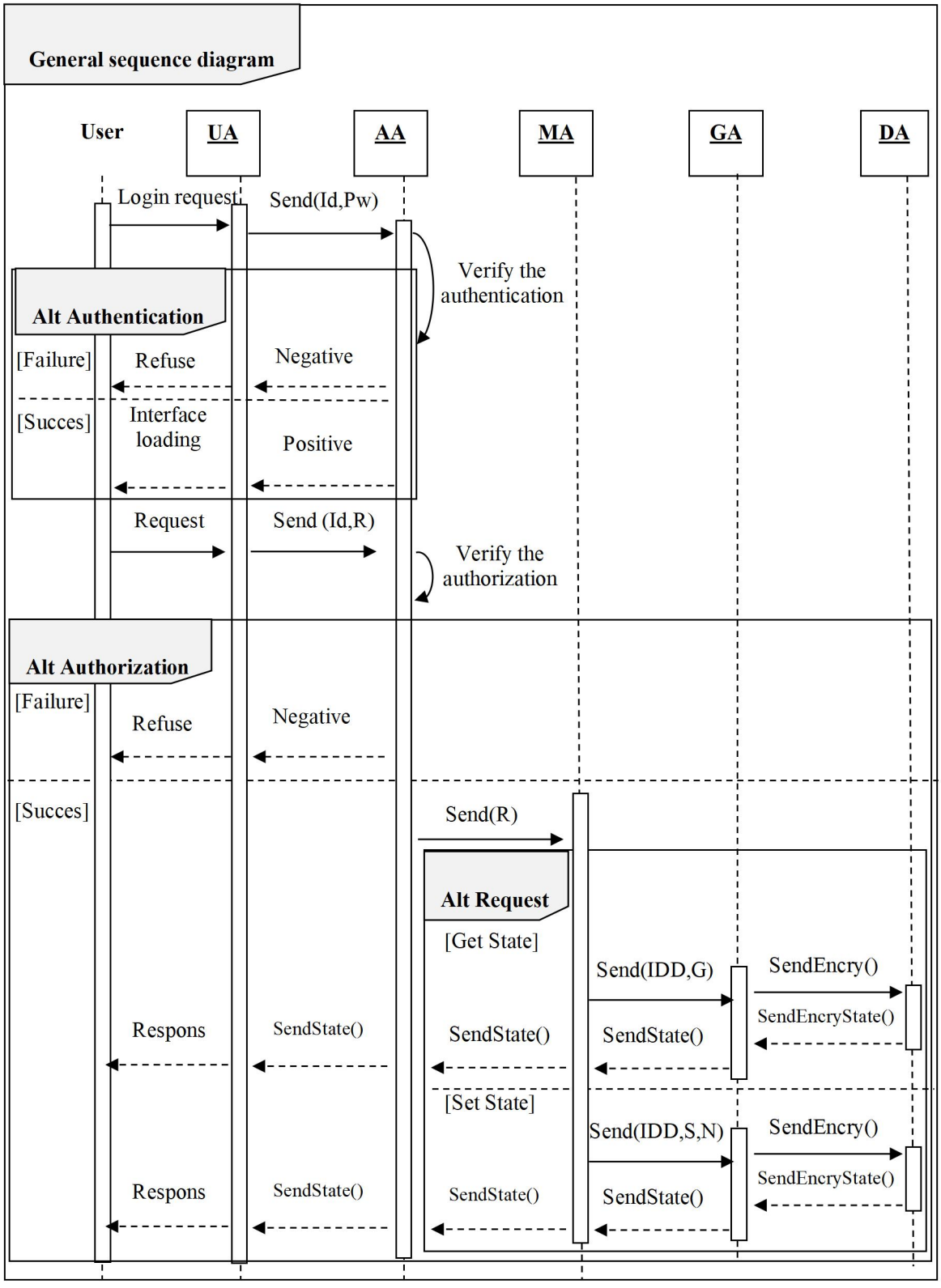

Figure 4.7. General diagram of interactions between agents [137].

4.5 Implementation and Results

In this section, we present the implementation and experimental process used to demonstrate the efficacy of the proposed system, including development tools, the case study, and the experimental results.

4.5.1 Development Tools

In order to ensure rapid and efficient development, proper functioning of our system based on agents, we have used two agent frameworks, osBrain for the device and Java Agent DEvelopment Framework (JADE) for the cloud and the mobile application.

- JADE: is free software distributed by Telecom Italia that was fully implemented with the JAVA programming language by the TILAB laboratory, intended for developers who want to build multi-agent systems [138]. A JADE-based architecture can be distributed across devices that do not even need to use the same operating system. The configuration can be controlled remotely through a graphical user interface (GUI), and when the agents are running, it can be changed by moving them from one device to another if required. In addition to the agent abstraction, JADE provides a simple but effective task execution and composition model. Also, JADE provides peer-to-peer agent communication based on the asynchronous message passing paradigm [139]. We have used JADE version 4.5.0. In addition to JADE, we used JADE-Android to develop agents in mobile applications, which is formed by the combination of the standard version of JADE and the android plug-in, intended for developers who are interested in creating JADE-based applications running on the Android Operating System [140].
- OsBrain: is free software Framework creation and execution agent that handles MAS in distributed environments such as IoT systems, fully implemented with the Python programming language by OpenSistemas. OsBrain agents operate autonomously and asynchronously communicate with each other through message passing. Remote agents may be treated and reconfigured even when they are running, not only variables but also new methods can be developed in remote agents [141]. We have used osBrain

platform version 0.6.5, which is based on the Python 3 programming language to build and run the agent that was embedded in the user device.

4.5.2 Case Study

In order to enhance the intelligence of our Cloud-IoT system for remote patient monitoring, described in the second chapter, we have integrated the agents in each layer, as shown in Figure 4.8. We have configured our agents for data analysis, and automatic real-time reasoning using parallelBehavior, which allows executing several behaviors in parallel to run code effectively and save time.

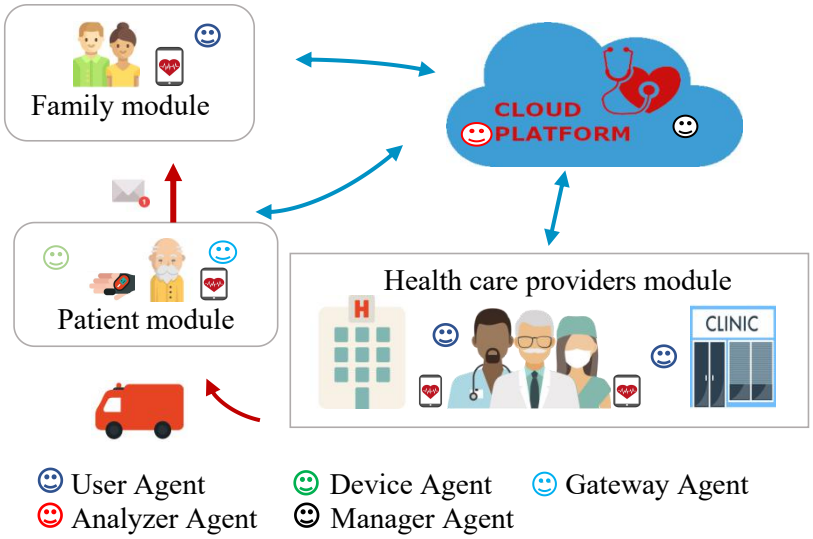

Figure 4.8. A Cloud-IoT health monitoring system based on smart.

Since the heart rate varies from person to person depending on factors like age, sex, and exercise, our algorithms are based on resting heart rate data from the Center for Disease Control and Prevention in the United States, shown in Table 4.2.

Table 4.2. Resting heart rate range [142].

Age group	Male	Female
4-5	87-104	84-100
6-8	79-94	76-92
9-11	76-91	70-86
12-15	70-87	70-87
16-19	69-85	66-83

Age group	Male	Female
20-39	66-82	61-78
40-59	64-79	61-77
60-79	64-78	60-75

- Device Agent: embedded agent in a wearable device prototype. The device agent can sense the heart rate, immediately send sensing data to the cloud, and securely communicate with the gateway agent in parallel.
- Gateway agent: embedded in the patient mobile application. It is responsible for data pre-treatment based on Table 4.2, detects the abnormal case, and sends a warning SMS to the healthcare providers and patient family if the patient's pulse is outside the normal range, and securely communicates with the other agents as shown in Figure 4.9.

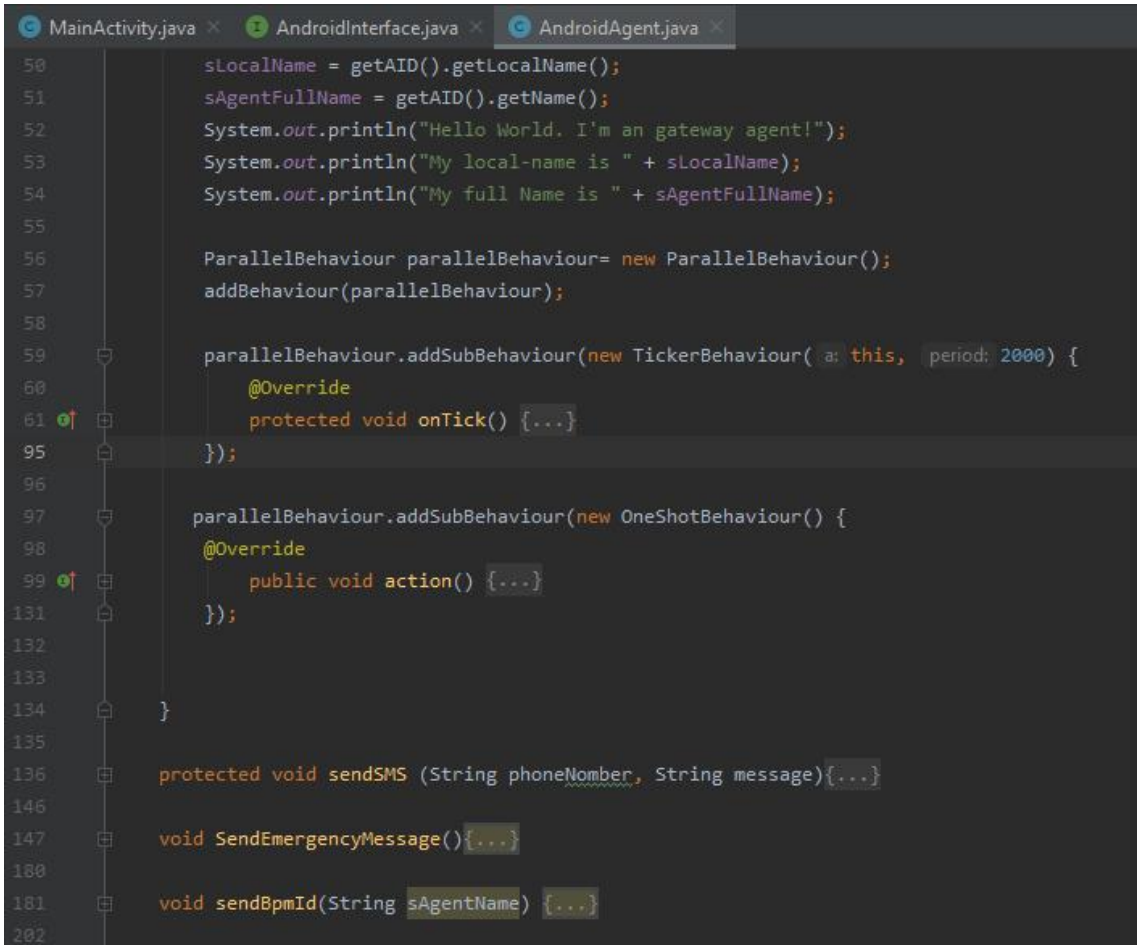

Figure 4.9. Smart device agent's algorithm.

- User agent: embedded in the medical staff mobile application. It does partial manipulation of the data based on Table 4.2, so if the patient's heartbeat is outside the normal level, the user agent changes the heart rate color to red color in the graphical interface. In addition to acquiring user requests and send/ receive those requests to the analyzer agent.
- Analyzer agent: embedded in the cloud, it is responsible for data analyzes (authorization and authorization) and request execution of the user. In addition to sends/receive requests to the user agent.
- Manager agent: embedded in the cloud, it is responsible for data collection, storing, processing, and data error detection.

4.6 Results and Discussion

Experiment results reveal that the proposed device can make fast and intelligent decisions in emergencies, launch the alarm to get help from the closest persons on the place and send an alarm message to the patient's family and the health care providers. As shown in Figure 4.10, the alarm message contains the patient's details, heart rate, and precise GPS coordinates. Thus, the health care providers take fast and appropriate decisions and apply the required actions to protect the patient life quickly.

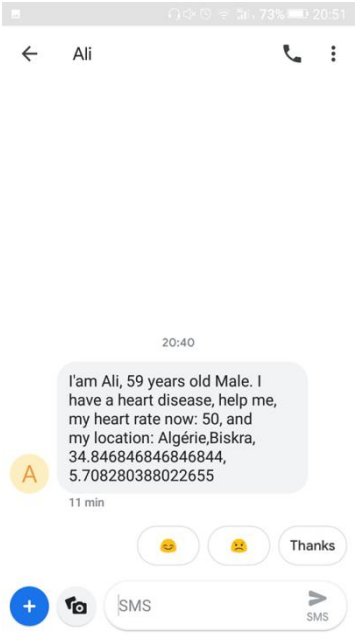

Figure 4.10. Alert message.

As shown in Figure 4.11, the real-time analysis of heart rate values helps the medical staff to know the patient's situation, prepare the appropriate manner for treating the patient, and take the appropriate decisions in emergency cases. The widespread adoption of this system can reduce the annual number of human deaths from cardiovascular disease.

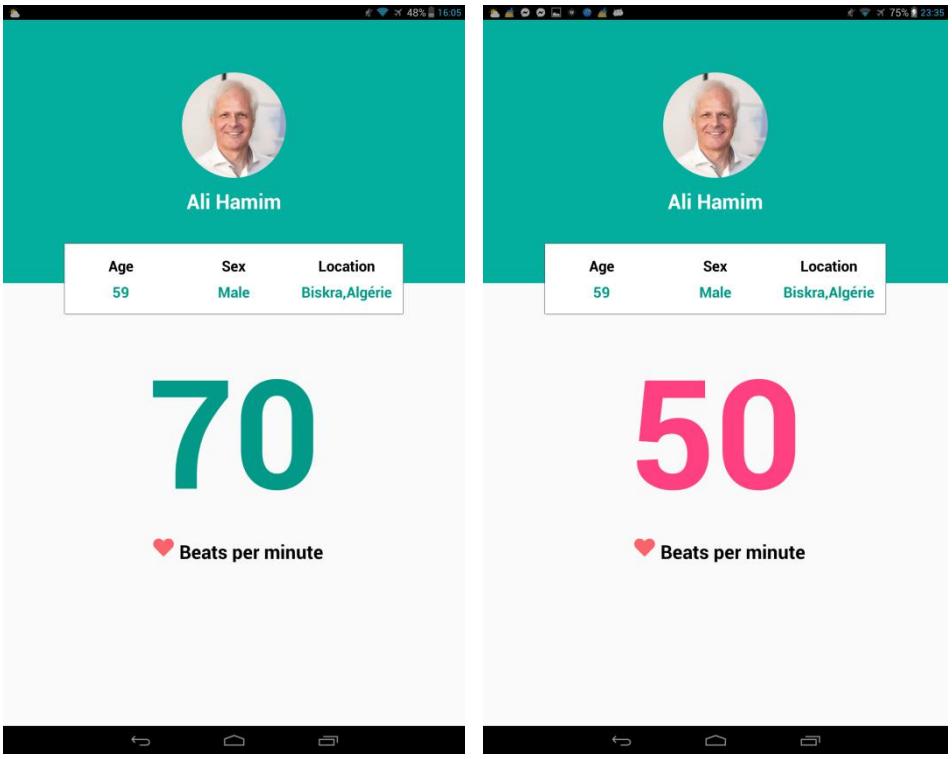

Figure 4.11. Accurate emergency case detection.

4.7 Conclusion

In this chapter, an integrated system that combines IoT and intelligent agent technology to enhance IoT intelligence has been proposed. The proposed system consists of a group of agents distributed in the four IoT architecture layers, as a vertical layer of agents; a group of agents collaborates to collect, process, and store data in the cloud. The remaining agents are deployed on IoT devices. We have configured our agents for data analysis and automatic real-time reasoning using parallel behavior, which allows executing several behaviors in parallel to run code effectively and save time. Experiment results reveal that the proposed system can make fast and intelligent decisions in emergencies without human intervention.

General Conclusion

Currently, IoT has gained wide popularity and attention thanks to its powerful applications in different fields. However, IoT technology is still facing several challenges that become more complicated with the huge increase in the number of connected devices to the Internet. In this regard, this thesis provided three main contributions. In the first contribution, we focused on the idea of integration between IoT and cloud computing technology to enhance the IoT ability of processing and storage with unlimited resources and capabilities of the cloud and improve IoT scalability. We have proposed a Cloud-IoT approach for real-time remote monitoring. In order to verify the validity of the proposed approach, we developed a Cloud-IoT system for remote patient monitoring. Healthy people can also benefit from the proposed system to check their health and wellness. Also, it helps the caregivers to easily measure and monitor patient heart rate anytime, anywhere for the pre-diagnosis of the patient's condition and early detection before the diseases develop into a crisis stage.

As a second contribution, we propose an integrated privacy protection system for IoT. The proposed system provided a high-performance and security level. It consists primarily of two phases: the first phase ensures data confidentiality in the perception layer based on lightweight cryptography. In the second phase, we have used the access control mechanism to ensure data privacy in the cloud through three steps: identification, authentication, and authorization. The experimentation demonstrates that the proposed solution more suitable for IoT devices that have computing and communication limits. In order to tap the most out of massive data streams, to enhance the intelligence of IoT devices, and to improve our first approach, we have developed an efficient, autonomous, and real-time solution based on the smart agent for data management and analysis in a secure way as a third contribution. The proposed system can collect, retrieve, store, and analyze the patient's heart rate securely. It can also detect the critical case immediately and take a quick and smart decision without requiring active human interaction.

Although the proposed framework is very promising and capable of providing very satisfactory results, there are other significant details that we want to carry out further in our future applications and research.

- Supporting patients' mobility by attaching a battery to the device and reduce the device's size.
- Developing the proposed system to meet other medical standards like ECG, body temperature, blood pressure, etc.
- Improve the agents' algorithm to predict and diagnose disease before it occurs, based on patients' physical information stored in a cloud.

List of Publications

International Journals

Ahmid, M., Kazar, O., Hamida, S., Kahloul, L., & Ghodous, P. (2015). Internet of Things New Challenges in Distributed Artificial Intelligence. International Journal of Computer Science and Electronics Engineering (IJCSEE), 3(5), 375-377.

Ahmid, M., Kazar, O., & Kahloul, L. (in press). A Secure and Intelligent Real-Time Health Monitoring System for Remote Cardiac Patients. International Journal of Medical Engineering and Informatics.

Ahmid, M., & Kazar, O. (in press). A Comprehensive Review of the Internet of Things Security. Journal of Applied Security Research (JASR).

International Conferences

Ahmid, M., Kazar, O., Hamida, S., Kahloul, L., & Ghodous, P. (2015, Novembre) An agent based approach for the Internet of Things. In 2nd International Workshop on Artificial Intelligence and Information & Communication Technologies (IWIICT 2015). Biskra, Algeria.

Ahmid, M., Kazar, O., Hamida, S., Kahloul, L., & Ghodous, P. (2015, December). Internet of Things New Challenges in Distributed Artificial Intelligence. In 2015 International Conference on Future Computational Technologies (ICFCT'2015) (pp. 158-162). Dubai, UAE.

Ahmid, M., Kazar, O., Benharzallah, S., Kahloul, L., & Merizig, A. (2020, February). An Intelligent and Secure Health Monitoring System Based on Agent. In 2020 International Conference on Informatics, IoT, and Enabling Technologies (ICIoT' 2020) (pp. 291-296). Doha, Qatar. IEEE.

Ahmid, M., & Kazar, O. (2021, July). A Cloud-IoT Health Monitoring System Based on Smart Agent for Cardiovascular Patients. In 2021 International Conference on Information Technology (ICIT 2021) (pp. 1-6). Amman, Jordan. IEEE.

National Conferences

Ahmid, M., Kazar, O., & Kahloul, L. (2017, Novembre). IoT and Security challenge. Doctoral Day LINFI (JDL'2017). Biskra, Algérie.

Ahmid, M., Kazar, O., & Kahloul, L. (2018, January). Une approche basée agent pour l'internet des objets. Journées d'Etudes Informatique Théorique et Appliquée (JEITA'2018). Biskra, Algeria.

REFERENCES

[1] Radenkovic, B., & Kocovic, P. (2020). From ubiquitous computing to the Internet of things. In Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications (pp. 1523-1556). IGI Global.

[2] Zhou, M., Fortino, G., Shen, W., Mitsugi, J., Jobin, J., & Bhattacharyya, R. (2016). Guest editorial special section on advances and applications of Internet of Things for smart automated systems. IEEE Transactions on Automation Science and Engineering, 13(3), 1225-1229.

[3] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. Information systems frontiers, 17(2), 261-274.

[4] Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. CISCO white paper, 1(2011), 1-11.

[5] Haller, S., Karnouskos, S., & Schroth, C. (2008, September). The internet of things in an enterprise context. In Future Internet Symposium (pp. 14-28). Springer.

[6] Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commision, 3(3), 34-36.

[7] Vannieuwenborg, F., Verbrugge, S., & Colle, D. (2018). Choosing IoT connectivity? A guiding methodology based on functional characteristics and economic considerations. Transactions on Emerging Telecommunications Technologies, 29(5), e3308.

[8] Xiao, G., Guo, J., Da Xu, L., & Gong, Z. (2014). User interoperability with heterogeneous IoT devices through transformation. IEEE Transactions on Industrial Informatics, 10(2), 1486-1496.

[9] Patel, K. K., & Patel, S. M. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. International journal of engineering science and computing, 6(5), 6122-6131.

[10] Forecast, G. M. D. T. (2019, February). Cisco visual networking index: global mobile data traffic forecast update, 2017–2022. CISCO white paper. (pp. 1-33).

[11] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.

[12] Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 83, 326-337.

[13] Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications, 24(3), 10-16.

[14] Sri, T. S., Prasad, J. R., & Vijayalakshmi, Y. (2016). A review on the state of art of Internet of Things. International Journal of Advanced Research in Computer and Communication Engineering, 5(7), 189-193.

[15] Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2015). Middleware for internet of things: a survey. IEEE Internet of things journal, 3(1), 70-95.

[16] Chelloug, S. A., & El-Zawawy, M. A. (2017). Middleware for internet of things: survey and challenges. Intelligent Automation & Soft Computing, 1-9.

[17] Asim, M. (2017). A survey on application layer protocols for Internet of Things (IoT). International Journal of Advanced Research in Computer Science, 8(3), 966-1000.

[18] Ahmid, M., Kazar, O., Hamida, S., Kahloul, L., & Ghodous, P. (2015). Internet of Things New Challenges in Distributed Artificial Intelligence. International Journal of Computer Science and Electronics Engineering (IJCSEE), 3(5), 375-377.

[19] Ahmid, M., Kazar, O., Benharzallah, S., Kahloul, L., & Merizig, A. (2020, February). An Intelligent and Secure Health Monitoring System Based on Agent. In 2020 International Conference on Informatics, IoT, and Enabling Technologies (ICIoT' 2020) (pp. 291-296). IEEE.

[20] Dey, N., Ashour, A. S., & Bhatt, C. (2017). Internet of things driven connected healthcare. In Internet of things and big data technologies for next generation healthcare (pp. 3-12). Springer, Cham.

[21] Jeong, H., Rogers, J. A., & Xu, S. (2020). Continuous on-body sensing for the COVID-19 pandemic: Gaps and opportunities. Science Advances, 6(36), eabd4794.

[22] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in industry, 101, 1-12.

[23] Mumtaz, S., Alsohaily, A., Pang, Z., Rayes, A., Tsang, K. F., & Rodriguez, J. (2017). Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation. IEEE Industrial Electronics Magazine, 11(1), 28-33.

[24] Robotics, A. B. B. (2019). YuMi—IRB 14000.

[25] Herrera-Quintero, L. F., Vega-Alfonso, J. C., Banse, K. B. A., & Zambrano, E. C. (2018). Smart its sensor for the transportation planning based on iot approaches using serverless and microservices architecture. IEEE Intelligent Transportation Systems Magazine, 10(2), 17-27.

[26] Ahmid, M., Kazar, O., Hamida, S., Kahloul, L., & Ghodous, P. (2015, December). Internet of Things New Challenges in Distributed Artificial Intelligence. In 2015 International Conference on Future Computational Technologies (ICFCT'2015) (pp. 158-162).

[27] Kim, T. H., Ramos, C., & Mohammed, S. (2017). Smart city and IoT. Future Generation Computer Systems, 76, 159-162

[28] Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., & Khoukhi, L. (2017). IoT technologies for smart cities. IET Networks, 7(1), 1-13.

[29] Schneider, S. (2017). The industrial internet of things (iiot) applications and taxonomy. Internet of Things and Data Analytics Handbook, 41-81.

[30] Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics, 14(11), 4724-4734.

[31] Solanki, A., & Nayyar, A. (2019). Green internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges. In Handbook of Research on Big Data and the IoT (pp. 379-405). IGI Global.

[32] Georgiou, K., Xavier-de-Souza, S., & Eder, K. (2017). The IoT energy challenge: A software perspective. IEEE Embedded Systems Letters, 10(3), 53-56.

[33] Lu, W., Gong, Y., Liu, X., Wu, J., & Peng, H. (2017). Collaborative energy and information transfer in green wireless sensor networks for smart cities. IEEE Transactions on Industrial Informatics, 14(4), 1585-1593.

[34] Mahapatra, C., Sheng, Z., Kamalinejad, P., Leung, V. C., & Mirabbasi, S. (2016). Optimal power control in green wireless sensor networks with wireless energy harvesting, wake-up radio and transmission control. IEEE Access, 5, 501-518.

[35] Radu, L. D. (2017). Green cloud computing: A literature survey. Symmetry, 9(12), 295.

[36] Mishra, S. K., Puthal, D., Sahoo, B., Jena, S. K., & Obaidat, M. S. (2018). An adaptive task allocation technique for green cloud computing. The Journal of Supercomputing, 74(1), 370-385.

[37] Pereira, C., & Aguiar, A. (2014). Towards efficient mobile M2M communications: Survey and open challenges. Sensors, 14(10), 19582-19608.

[38] Oncel, S. S. (2017). Green energy engineering: Opening a green way for the future. Journal of cleaner production, 142, 3095-3100.

[39] Gibson, L., Wilman, E. N., & Laurance, W. F. (2017). How green is ‘green’energy?. Trends in ecology & evolution, 32(12), 922-935.

[40] Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. Information Security Journal: A Global Perspective, 27(3), 162-182.

[41] Enterprise, H. P. (2015). Internet of things research study: 2015 report. Online: http://www8. hp. com/h20195, 2.

[42] Ahmid, M., & Kazar, O. (in press). A Comprehensive Review of the Internet of Things Security. Journal of Applied Security Research (JASR).

[43] Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. Future Generation Computer Systems, 100, 144-164.

[44] Ali, F., Khan, M. S., & Akhtar, H. (2019). Security Review in Internet of Things. Internet of Things and Cloud Computing, 7(3), 80-87.

[45] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: A survey. Journal of Healthcare Engineering, 2019, 1-16.

[46] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42.

[47] Bhushan, K., & Gupta, B. B. (2017). Security challenges in cloud computing: state-of-art. International Journal of Big Data Intelligence, 4(2), 81-107.

[48] Lu, Y., & Da Xu, L. (2018). Internet of things (iot) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115.

[49] Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future generation computer systems, 108, 909-920.

[50] Aazam, M., & Huh, E. N. (2016). Fog computing: The cloud-iot\/ioe middleware paradigm. IEEE Potentials, 35(3), 40-44.

[51] Kobusińska, A., Leung, C., Hsu, C. H., Raghavendra, S., & Chang, V. (2018). Emerging trends, issues and challenges in Internet of Things, Big Data and cloud computing. Future Generation Computer Systems, 87, 416-419.

[52] Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2016). IoT-based big data storage systems in cloud computing: perspectives and challenges. IEEE Internet of Things Journal, 4(1), 75-87.

[53] Jirkovský, V., Obitko, M., & Mařík, V. (2016). Understanding data heterogeneity in the context of cyber-physical systems integration. IEEE Transactions on Industrial Informatics, 13(2), 660-667.

[54] Rashid, Z. N., Zebari, S. R., Sharif, K. H., & Jacksi, K. (2018, October). Distributed Cloud Computing and Distributed Parallel Computing: A Review. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 167-172). IEEE.

[55] Javaid, N., Sher, A., Nasir, H., & Guizani, N. (2018). Intelligence in IoT-based 5G networks: Opportunities and challenges. IEEE Communications Magazine, 56(10), 94-100.

[56] Zhang, Y., Ma, X., Zhang, J., Hossain, M. S., Muhammad, G., & Amin, S. U. (2019). Edge intelligence in the cognitive Internet of Things: Improving sensitivity and interactivity. IEEE Network, 33(3), 58-64.

[57] Mohamed, E. (2020). The Relation of Artificial Intelligence with Internet Of Things: A survey. Journal of Cybersecurity and Information Management, 1(1), 30-24.

[58] González García, C., Núñez Valdéz, E. R., García Díaz, V., Pelayo García-Bustelo, B. C., & Cueva Lovelle, J. M. (2019). A review of artificial intelligence in the Internet of Things. International Journal of Interactive Multimedia and Artificial Intelligence, 5, 9-20.

[59] Ghosh, A., Chakraborty, D., & Law, A. (2018). Artificial intelligence in Internet of things. CAAI Transactions on Intelligence Technology, 3(4), 208-218.

[60] Scully, P. (2020). Top 10 IoT applications in 2020. Retrieved from https://iot-analytics.com/top-10-iot-applications-in-2020/

[61] O'Dea, S. (2020). Data volume of IoT connected devices worldwide 2019 and 2025. Retrieved from https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size/

[62] O'Dea, S. (2020). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. Retrieved from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[63] Forkan, A., Khalil, I., & Tari, Z. (2014). CoCaMAAL: A cloud-oriented context-aware middleware in ambient assisted living. Future Generation Computer Systems, 35, 114-127.

[64] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[65] Psannis, K. E., Xinogalos, S., & Sifaleras, A. (2014). Convergence of Internet of things and mobile cloud computing. Systems Science & Control Engineering: An Open Access Journal, 2(1), 476-483.

[66] Jadhav, S. R., Shinde, R. P., Patil, P. S., Thakar, G. B. (2018). Health Detector Android Application using IoT for Rural Area. International Journal on Future Revolution in Computer Science & Communication Engineering, 4(5), 131-136.

[67] Fu, Y., & Liu, J. (2015). System design for wearable blood oxygen saturation and pulse measurement device. Procedia manufacturing, 3, 1187-1194.

[68] Vuha, C. A. H. K., Rajani, M., & Vineeth, J. M. (2017). Smart Health Care Monitoring using Internet of Things and Android. International Journal of Advanced Research in Electronics and Communication Engineering, 6(3), 101-104.

[69] Navdeti, P., Parte, S., Talashilkar, P., Patil, J., & Khairnar, V. (2016). Patient parameter monitoring system using Raspberry Pi. International Journal Of Engineering And Computer Science, 5(3).

[70] Reddy, N. A., Krishnan, G. H., & Raghuram, D. (2016). Real Time Patient Health Monitoring Using Raspberry PI. Research Journal of Pharmaceutical Biological And Chemical Sciences, 7(6), 570-575.

[71] Kakria, P., Tripathi, N. K., & Kitipawang, P. (2015). A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors. International journal of telemedicine and applications, 2015, 1-11.

[72] Aminian, M., & Naji, H. R. (2013). A hospital healthcare monitoring system using wireless sensor networks. International Journal of Health & Medical Informatics, 4(02), 121.

[73] Aranki, D., Kurillo, G., Yan, P., Liebovitz, D. M., & Bajcsy, R. (2016). Real-time tele-monitoring of patients with chronic heart-failure using a smartphone: Lessons learned. IEEE Transactions on Affective Computing, 7(3), 206-219.

[74] Suprayitno, E. A., Marlianto, M. R., & Mauliana, M. I. (2019). Measurement device for detecting oxygen saturation in blood, heart rate, and temperature of human body. In Journal of Physics, 1402(3), 1-6.

[75] Jovanov, E., Lords, A. D., Raskovic, D., Cox, P. G., Adhami, R., & Andrasik, F. (2003). Stress monitoring using a distributed wireless intelligent sensor system. IEEE Engineering in Medicine and Biology Magazine, 22(3), 49-55.

[76] Paradiso, R., Loriga, G., & Taccini, N. (2005). A wearable health care system based on knitted integrated sensors. IEEE transactions on Information Technology in biomedicine, 9(3), 337-344.

[77] Kwon, S., Lee, D., Kim, J., Lee, Y., Kang, S., Seo, S., & Park, K. (2016). Sinabro: A smartphone-integrated opportunistic electrocardiogram monitoring system. Sensors, 16(3), 361.

[78] Malhi, K., Mukhopadhyay, S. C., Schnepper, J., Haefke, M., & Ewald, H. (2012). A zigbee-based wearable physiological parameters monitoring system. IEEE sensors journal, 12(3), 423-430.

[79] Lee, J. V., Chuah, Y. D., & Chieng, K. T. (2013). Smart elderly home monitoring system with an android phone. International Journal of Smart Home, 7(3), 17-32.

[80] Suma, N., Samson, S. R., Saranya, S., Shanmugapriya, G., & Subhashri, R. (2017). IOT based smart agriculture monitoring system. International Journal on Recent and Innovation Trends in computing and communication, 5(2), 177-181.

[81] Gondchawar, N., & Kawitkar, R. S. (2016). IoT based smart agriculture. International Journal of advanced research in Computer and Communication Engineering, 5(6), 838-842.

[82] Yan, M., & Shi, H. (2013). Smart living using Bluetooth-based Android smartphone. International journal of wireless & mobile networks, 5(1), 65.

[83] Javale, D., Mohsin, M., Nandanwar, S., & Shingate, M. (2013). Home automation and security system using Android ADK. International journal of electronics communication and computer technology (IJECCT), 3(2), 382-385.

[84] Jagannathan, S., & Priyatharshini, R. (2015, July). Smart farming system using sensors for agricultural task automation. In 2015 IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR) (pp. 49-53). IEEE.

[85] Kaewmard, N., & Saiyod, S. (2014, October). Sensor data collection and irrigation control on vegetable crop using smart phone and wireless sensor networks for smart farm. In 2014 IEEE Conference on Wireless Sensors (ICWiSE) (pp. 106-112). IEEE.

[86] Cardiovascular Diseases. (2017, May 17). WHO. Retrieved from https://www.who.int/health-topics/cardiovascular-diseases/#tab=tab_1

[87] Medical doctors (per 10 000 population). (2015, October 20). WHO. Retrieved from https://www.who.int/data/gho/data/indicators/indicator-details/GHO/medical-doctors-(per-10-000-population)

[88] Smyth, N. (2017). Android Studio 2.3 Development Essentials-Android 7 Edition. PayloadMedia, Inc..

[89] Stonehem, B. (2016). Google Android Firebase: Learning the Basics (Vol. 1). First Rank Publishing.

[90] Upton, E., & Halfacree, G. (2014). Raspberry Pi user guide. John Wiley & Sons.

[91] Lindberg, L. G., Tamura, T., & Öberg, P. Å. (1991). Photoplethysmography. Medical and Biological Engineering and Computing, 29(1), 40-47.

[92] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities, 78(2), 544-546.

[93] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.

[94] Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11), 20-26.

[95] Maras, M. H. (2015). Internet of Things: security and privacy implications. International Data Privacy Law, 5(2), 99-104.

[96] Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A privacy preserving communication protocol for IoT applications in smart homes. IEEE Internet of Things Journal, 4(6), 1844-1852.

[97] Rghioui, A., L'aarje, A., Elouaai, F., & Bouhorma, M. (2014, October). The internet of things for healthcare monitoring: security review and proposed solution. In 2014 Third IEEE International Colloquium in Information Science and Technology (CIST) (pp. 384-389). IEEE.

[98] Gong, T., Huang, H., Li, P., Zhang, K., & Jiang, H. (2015, December). A medical healthcare system for privacy protection based on IoT. In 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP) (pp. 217-222). IEEE.

[99] Gope, P., & Hwang, T. (2015). BSN-Care: A secure IoT-based modern healthcare system using body sensor network. IEEE sensors journal, 16(5), 1368-1376.

[100] Kulkarni, S., Durg, S., & Iyer, N. (2016, March). Internet of things (iot) security. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 821-824). IEEE.

[101] Shafagh, H., Hithnawi, A., Dröscher, A., Duquennoy, S., & Hu, W. (2015, November). Talos: Encrypted query processing for the internet of things. In Proceedings of the 13th ACM conference on embedded networked sensor systems (pp. 197-210). ACM.

[102] Alharbi, K. N., Lin, X., & Shao, J. (2016). A privacy-preserving data-sharing framework for smart grid. IEEE Internet of Things Journal, 4(2), 555-562.

[103] Doukas, C., Maglogiannis, I., Koufi, V., Malamateniou, F., & Vassilacopoulos, G. (2012, November). Enabling data protection through PKI encryption in IoT m-Health devices. In 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE) (pp. 25-29). IEEE.

[104] Nguyen, K. T., Oualha, N., & Laurent, M. (2018). Securely outsourcing the ciphertext-policy attribute-based encryption. World Wide Web, 21(1), 169-183.

[105] Thirumalai, C., & Kar, H. (2017, April). Memory Efficient Multi Key (MEMK) generation scheme for secure transportation of sensitive data over Cloud and IoT devices. In 2017 Innovations in Power and Advanced Computing Technologies (i-PACT) (pp. 1-6). IEEE.

[106] Guo, A., Xu, M., Ran, F., & Wang, H. (2019). A novel medical internet of things perception system based on visual image encryption and intrusion detection. Cluster Computing, 22(6), 13405-13413.

[107] Zhang, H., Yu, J., Tian, C., Tong, L., Lin, J., Ge, L., & Wang, H. (2020). Efficient and secure outsourcing scheme for RSA decryption in Internet of Things. IEEE Internet of Things Journal, 7(8), 6868-6881.

[108] Barker, E., & Dang, Q. (2016). Nist special publication 800-57 part 1, revision 4. NIST, Tech. Rep, 16.

[109] Arsénio, A., Serra, H., Francisco, R., Nabais, F., Andrade, J., & Serrano, E. (2014). Internet of intelligent things: Bringing artificial intelligence into things and communication networks. In Inter-cooperative collective intelligence: Techniques and applications (pp. 1-37). Springer, Berlin, Heidelberg.

[110] Hu, F., Xie, D., & Shen, S. (2013, August). On the application of the internet of things in the field of medical and health care. In 2013 IEEE international conference on green computing and communications and IEEE Internet of Things and IEEE cyber, physical and social computing (pp. 2053-2058). IEEE.

[111] Blake, M. B. (2015). An internet of things for healthcare. IEEE Annals of the History of Computing, 19(04), 4-6.

[112] Dimitrov, D. V. (2016). Medical internet of things and big data in healthcare. Healthcare informatics research, 22(3), 156.

[113] Ferber, J. (1997). Les systèmes multi-agents: vers une intelligence collective. InterEditions.

[114] Jennings, N. R., & Wooldridge, M. (1998). Applications of intelligent agents. In Agent technology (pp. 3-28). Springer, Berlin, Heidelberg.

[115] Jennings, N. R. (2000). On agent-based software engineering. Artificial intelligence, 117(2), 277-296.

[116] Russell, S., & Norvig, P. (2010). Intelligence artificielle: Avec plus de 500 exercices. Pearson Education France.

[117] Suzanne Barber, K., Goel, A., & Martin, C. E. (2000). Dynamic adaptive autonomy in multi-agent systems. Journal of Experimental & Theoretical Artificial Intelligence, 12(2), 129-147.

[118] d'Inverno, M., Luck, M., Georgeff, M., Kinny, D., & Wooldridge, M. (2004). The dMARS architecture: A specification of the distributed multi-agent reasoning system. Autonomous Agents and Multi-Agent Systems, 9(1), 5-53.

[119] Ferber, J., & Weiss, G. (1999). Multi-agent systems: an introduction to distributed artificial intelligence. Reading: Addison-Wesley.

[120] Huhns, M. N., & Singh, M. P. (1998). Cognitive agents. IEEE Internet computing, 2(6), 87-89.

[121] Cruces, A. L. L., & De Arriaga, F. (2000). Reactive agent design for intelligent tutoring systems. Cybernetics & Systems, 31(1), 1-47.

[122] Nwana, H. S. (1996). Software agents: An overview. Knowledge engineering review, 11(3), 205-244.

[123] Sycara, K. P. (1998). Multiagent systems. AI magazine, 19(2), 79-79.

[124] Dorri, A., Kanhere, S. S., & Jurdak, R. (2018). Multi-agent systems: A survey. Ieee Access, 6, 28573-28593.

[125] Fortino, G., Guerrieri, A., Russo, W., & Savaglio, C. (2014, May). Integration of agent-based and cloud computing for the smart objects-oriented IoT. In Proceedings of the 2014 IEEE 18th international conference on computer supported cooperative work in design (CSCWD) (pp. 493-498). IEEE.

[126] Vaidehi, V., Vardhini, M., Yogeshwaran, H., Inbasagar, G., Bhargavi, R., & Hemalatha, C. S. (2013). Agent based health monitoring of elderly people in indoor environments using wireless sensor networks. Procedia Computer Science, 19, 64-71.

[127] Polu, S. K. (2019). Modeling of efficient multi-agent based mobile health care system. Int J Innov Res Sci Technol, 5(8), 10-14.

[128] Su, C. J., & Wu, C. Y. (2011). JADE implemented mobile multi-agent based, distributed information platform for pervasive health care monitoring. Applied Soft Computing, 11(1), 315-325.

[129] Naranjo-Hernández, D., Roa, L. M., Reina-Tosina, J., & Estudillo-Valderrama, M. Á. (2012). SoM: A smart sensor for human activity monitoring and assisted healthy ageing. IEEE transactions on biomedical engineering, 59(11), 3177-3184.

[130] Santos, J., Rodrigues, J. J., Silva, B. M., Casal, J., Saleem, K., & Denisov, V. (2016). An IoT-based mobile gateway for intelligent personal assistants on mobile health environments. Journal of Network and Computer Applications, 71, 194-204.

[131] Chan, V., Ray, P., & Parameswaran, N. (2008). Mobile e-Health monitoring: an agent-based approach. IET communications, 2(2), 223-230.

[132] Smarsly, K., Law, K. H., & Hartmann, D. (2012). Multiagent-based collaborative framework for a self-managing structural health monitoring system. Journal of computing in civil engineering, 26(1), 76-89.

[133] Sharma, A., Srinivasan, D., & Kumar, D. S. (2016, July). A comparative analysis of centralized and decentralized multi-agent architecture for service restoration. In 2016 IEEE congress on evolutionary computation (CEC) (pp. 311-318). IEEE.

[134] Su, C. J., & Chu, T. W. (2014). A mobile multi-agent information system for ubiquitous fetal monitoring. International journal of environmental research and public health, 11(1), 600-625.

[135] Al-Sakran, H. O. (2015). Intelligent traffic information system based on integration of Internet of Things and Agent technology. International Journal of Advanced Computer Science and Applications (IJACSA), 6(2), 37-43.

[136] Ahmid, M., & Kazar, O. (2021, July). A Cloud-IoT Health Monitoring System Based on Smart Agent for Cardiovascular Patients. In 2021 International Conference on Information Technology (ICIT 2021) (pp. 1-6). IEEE.

[137] Ahmid, M., Kazar, O., & Kahloul, L. (in press). A Secure and Intelligent Real-Time Health Monitoring System for Remote Cardiac Patients. International Journal of Medical Engineering and Informatics.

[138] Chmiel, K., Gawinecki, M., Kaczmarek, P., Szymczak, M., & Paprzycki, M. (2005). Efficiency of JADE agent platform. Scientific Programming, 13(2), 159-172.

[139] Bellifemine, F., Poggi, A., & Rimassa, G. (2000, July). Developing multi-agent systems with JADE. In International Workshop on Agent Theories, Architectures, and Languages (pp. 89-103). Springer, Berlin, Heidelberg.

[140] Bergenti, F., Caire, G., & Gotta, D. (2014, September). Agents on the Move: JADE for Android Devices. WOA, 1260, 1-5.

[141] osBrain. (2019). What is osBrain?. Available at: https://osbrain.readthedocs.io/en/stable/ (accessed 12 August 2019)

[142] Ostchega, Y. (2011). Resting pulse rate reference data for children, adolescents, and adults: United States. US Department of Health and Human Services, Centers for Disease Control and Prevention, National Center for Health Statistics.