Providing a Framework for Security Management in Internet of Things

XUE Zhen*, LIU Xingyue
School of Management
China University of Mining and Technology-Beijing
Beijing, 100083, China

***Abstract*—With the advent of Internet of Things technology, tremendous changes are taking place. Perhaps what humans never even imagined will come in the near future, and just as the Internet surrounds all aspects of people's daily lives, intelligent objects will autonomously take over all aspects of people's lives. So far, a lot of research and development has been done in the field of Internet of Things, but there are still many challenges in this field. One of the most important challenges is the issue of security in the Internet of Things. Therefore, in this paper, while reviewing the requirements, models and security architectures of the Internet of Things, a framework for security management in the Internet of Things is proposed, which takes into account various aspects and requirements. The proposed framework uses various ideas such as cryptography, encryption, anomaly detection, intrusion detection, and behavior pattern analysis and can be considered as a basis for future research. The purpose of this research is to determine security requirements and provide a method to improve security management in the Internet of Things. Based on the tests, the proposed method is completely 100% resistant against data modification attacks. Against impersonation attacks up to 97% and against denial of service attacks up to 89% resistant detection accuracy.**

***Keywords*—Internet of Things (IoT); security management; security requirement; security model; security architecture**

I. INTRODUCTION

Internet of Things (IoT) is a new concept in the world of technology and communication. The term Internet of Things was first used in 1999 by Kevin Ashton. He described a world in which everything, including inanimate objects, would have a digital identity of their own, allowing computers to organize and manage them. The Internet currently connects all people, but with the IoT, all things are connected. In other words, the Internet of Things is a modern technology in which any entity (human, animal, or objects) can send data through communication networks, either the Internet or intranet [1, 2].

According to Cisco research, the birth of the Internet of Things is estimated between 2008 and 2009. This research also shows that after 2008, the number of devices connected to the Internet is more than the total number of human population and their number is increasing exponentially. Thus, it is predicted that by 2030, the number of devices connected to the Internet will reach more than 30 billion IoT devices in the world [3, 4]. In research communities, the Internet of Things has been defined from different aspects and perspectives; therefore, several definitions have been provided for it. The difference of different views is rooted in the two terms "Internet" and "things". The first (internet-oriented) perspective moves the IoT perspective to a network-oriented perspective, and the second (object-oriented) perspective shifts the main focus to public objects that must be integrated into a common framework [5]. But in the field of information and communication, the terms "Internet" and "things" when used together, evoke a new concept. From a semantic point of view, the Internet of Things means "a wide global network, based on standard communication protocols, of interconnected objects, each of which can be uniquely addressed" [4]. Right now, the Internet of Things has evolved from a random collection of purpose-built networks. For example, today's cars have multiple networks to control engine performance, safety features, communication systems, etc. Commercial and residential buildings also have different control systems for cooling, heating and air conditioning, telephone service, security and lighting. With the progress and evolution of the Internet of Things, these networks and many other networks will be connected to each other with additional management, analysis and security capabilities. This issue will increase the power of the IoT [2]. The potential possibilities offered by the Internet of Things make it possible to use it in many applications. But currently there is only a small part of its applications in society. Nevertheless, in many different contexts and environments, the use of new applications is likely to improve people's quality of life. As an example, can refer to its various uses at home, when traveling, and also its various uses at work, when sick. These environments are now equipped with various objects that have a basic intelligence. But in most cases, these objects do not have any communication capabilities. Creating the ability to communicate with each other, for these objects, and enriching the information received from the surrounding environment, implies that there are different environments in which a very wide range of applications can be deployed [3]. Many challenges have arisen with the emergence of the Internet of Things. These challenges can be examined from different aspects, including social and technical. As an example, can mention security challenges [5] and legal challenges [6]. In order to accept and spread the Internet of Things, its challenges must be well identified and overcome [7]. One of the limitations of this study is low power and few resources, which is not always possible due to the implementation of complex security algorithms on Internet of Things systems. Security management is one of the basic security challenges in the Internet of Things, and this issue is very important and necessary for the development of this emerging technology.

*Corresponding Author.

Despite this issue, the activities carried out so far have not been able to provide a complete and appropriate answer to this issue. Therefore, further research in this regard can contribute to the development of the frontiers of knowledge and finally, provide new horizons for the development and applications of the Internet of Things. Therefore, in this research, an effort will be made to propose a suitable solution for security management, while reviewing the literature on the subject and determining the security requirements of the Internet of Things, which will ultimately lead to improvements in this field and also to improve the level of security in the Internet of Things. Since in this paper focus is on the security challenges of the Internet of Things. In the continuation of this paper, security requirements, security models and security architectures of the Internet of Things are examined first, and then a framework for managing security in the Internet of Things is presented.

- The following questions are raised in this research:
- What are the security requirements of the Internet of Things?
- How to meet the security requirements of the Internet of Things?
- How to provide a method to improve security management in the Internet of Things?

In the following, Paper is configured as follows. In Section II, the requirements of the Internet of Things in different environments are discussed. Sections III and IV deal with security models and architectures in the Internet of Things. In Section V, the framework of the proposed method for managing security in the Internet of Things is presented, and finally, 6 is related to the conclusion.

II. Related Work

Users can ensure that they have a secure, private place with the aid of data security. The centralized administration of data security across several Internet of Things levels is the subject of this study. The compliance standard, identity management, data management, policy engine, and audit reports are the key axes of this paper. Standards for security, hardware security, adherence to certain legislation, and flaws in the IoT layer are not demonstrated in this paper [8]. The Internet of Things has numerous advantages, but it also faces significant difficulties. The most crucial of them is raising an IoT network's vital connections' susceptibility to hacker attacks. There is currently no tested access control technique for designing security frameworks with device authentication. This issue has been resolved in the source [9] of the method of expanding a security framework with powerful and transparent security protection. These issues involve creating new authentication mechanisms, an access control subsystem, and extremely precise risk indicators, as well as looking at the security requirements of three scenarios, including IoT of the body, IoT for the home, and IoT for the hotel. The sample security framework provided provides us with some workable answers to some of the security issues associated with the Internet of Things. In source [10], researchers looked into the traits of seven well-known frameworks in an effort to make choosing a good framework for an industrial application easier. The choice of a suitable framework is complicated by the growing number of frameworks and platforms that already exist and offer varying degrees of support for the aforementioned needs. It takes effort. The goal of this study is to highlight new developments in existing research and the most recent commercial Internet of Things frameworks, as well as to provide a technical comparison of their traits. An examination of the Internet of Things' current state and security issues is provided by source [11]. (IoT). Connecting people to anything and anywhere is one of the objectives of the IoT framework. Perception, Network, and Application layers make up the three-layer architecture that characterizes the Internet of Things. Therefore, in order to fulfill Internet of Things goals that have a high reliability factor, a variety of security principles must be applied in each layer. Only if the security concerns related to the IoT framework are resolved can its future be assured. Many researchers have attempted to design appropriate countermeasures in order to solve the unique security issues of IoT layers and devices. In order to secure the Internet of Things, this paper presents an overview of security principles, technological and security concerns, possible solutions, and future perspectives. IACS will undergo architectural modifications as a result of the acceptance and deployment of Internet of Things (IoT) technologies, including improved connectivity to industrial systems. The growth of IoT technologies in industrial systems has altered the IACS architecture by adding more connections inside the chips. Industry 4.0 and physical-cyber systems have both been looked at in the paper [12]. This paper defines the IIoT and examines the associated IoT subcategories. In order to count and characterize IIoT devices when examining system design and security threats and vulnerabilities, it offers an analytical framework for IIoT. The conclusion of this research identifies certain gaps in the literature. In [13], a framework for blockchain-based GSD public access control is given, offering users a platform for comprehensive GSD administration. First, users and GSDs issue visual identities based on the World Wide Web Consortium (W3C) Decentralized Identifiers standard (VIDs). Then, they added user and device authentication to the GSD-DIDs protocol. Finally, an integrated access control system for GSD was created based on the decentralization and non-tampering characteristics of blockchain. This system comprises registering, granting, and cancelling access privileges.Using this framework, users can accomplish decentralized, lightweight, and fine-grained GSD access control, according to the findings of the experiments. The research [14] introduces the information security risks the Internet of Energy faces, classifies errors, and studies the information security defenses of distributed energy stations operating in the Internet of Energy environment. This paper analyzes the countermeasures to protect the distributed energy station's information security, analyzes the security framework of the distributed energy station by building the network security framework, and presents the system architecture of the distributed energy station in the Internet of Energy environment in accordance with its network security features. The study [15] employed a systematic literature review (SLR) technique and went through all of the basic literature to look for structures and themes. These approaches were carried out in four steps: eligibility, screening, identification, and so on.

After 568 papers from reliable journals were evaluated, 260 papers and 54 reports were analyzed. Additionally, they used MAXQDA to conduct an analysis in which nodes and themes were first discovered. A qualitative model was created using MAXQDA after classification. The proposed paradigm has literary backing, making it beneficial for IoT consumers, developers, and IT managers. In order to balance security and other services in dense IoT, an ascending authentication framework (AAF) is presented in [16]. Through integrated keying and allocation, the proposed system offers a high level of authentication and user services. A framework that includes service providers and end users defines this procedure. In this authentication, key distribution follows a discrete assignment method while service authentication uses hyperelliptic curve cryptography. Regression learning is used to determine the discontinuity and continuity in authentication in this case. For future service releases, the level of authentication and security redemption is determined by a modification in the distribution function. As a result, the regression sequence is completely altered without the inclusion of any new keys. This lowers failure rates, response latency, service authentication time, and computational complexity. In order to study the use of IoT in diabetes monitoring, critical issues, a systematic literature analysis on the adoption of MHIoT for diabetes management was undertaken in [17] Methodology comprehensive literature review. Despite the larger benefits of MHIoT in such resource-constrained environments, key studies show that underdeveloped countries are falling behind. Findings indicate that the biggest barriers to MHIoT adoption for diabetes control are infrastructure costs, security concerns, and privacy concerns. As healthcare costs decline in a context of limited resources, the opportunities afforded by MHIoT exceed the constraints. To fully reap these benefits and handle problems, more study is needed on infrastructure needs and privacy issues. The paper [18] presents trustworthy algorithms for the Internet of Things' security framework. On actual marketing data for the bank obtained from the Cloud Internet of Things, these algorithms, which include Simple Bayes (NB), Logistic Regression (LR), Random Forest (RF), Support Vector Machine (SVM), ID3, and C4.5, are applied (CIoT). By identifying the key factors influencing success and evaluating the effectiveness of CIoT and SDM algorithms, this study aims to develop an effective framework for improving marketing campaigns for banks. This work is anticipated to boost scientific contributions in researching marketing information capabilities by merging SDM with CIoT. There are eight factors used to calculate how well SDM algorithms perform. Precision, balance precision, accuracy, root mean absolute error, recall, F1-score, and run time. Experimental results demonstrate the success of the suggested framework, which has higher accuracy and good performance. The findings demonstrated the importance of marketing strategies and customer service to a company's success and survival.

III. Internet of Things Security Requirements

To implement security in any system in the Internet of Things, different areas such as environment, user, software, physical device, information and network should be considered in an integrated manner and in the form of a general solution. In other words, paying attention to each of these areas alone cannot be a guarantee for creating and establishing security in the Internet of Things, but requires an answer that considers all these areas in a comprehensive and integrated manner [19, 28]. To protect communications in IoT, sufficient assurance in terms of confidentiality, integrity, authentication and non-repudiation of information flow must be provided. The security of Internet of Things communication can be considered in the context of communication protocols. Also, this work can be done with external mechanisms and on the other side of communication. Other security requirements must also be considered for the Internet of Things. In particular, by considering the communication between objects, it can be concluded that attacks such as denial of service can target data availability. Therefore, there is a need for mechanisms to protect against such threats that guarantee the proper functioning of IoT communication protocols. Other security requirements of the IoT include privacy, anonymity, responsibility, and trust, which are necessary for the social acceptance of most future applications of the IoT [20, 35, 27]. Security key management is another important security requirement in the field of Internet of Things. In particular, due to the fact that the security keys are accessible to attackers, if an attacker gets hold of these keys, he will be able to recover all the information being sent by the relevant device. In addition to key management, there is a need for appropriate methods for generating, distributing, exchanging, updating and revoking keys. Appropriate encryption protocols and mechanisms should also be used. IoT devices are expected to operate unattended and deploy in unprotected environments. Subsequently, this makes IoT devices easily accessible to attackers and increases the risk of physical attacks on them. Therefore, there is a need for mechanisms to prevent interference and attacks related to hardware elements and embedded chips in IoT devices [21, 36]. Generally, the security requirements in the IoT can be examined and analyzed from different aspects. In this research, based on the studies, a complete list of security requirements in the field of IoT has been prepared and shown in Table I. In addition, each of these requirements are also placed in a special category. This table can be used to develop security models and architectures and propose new frameworks to improve security management in the IoT, which will ultimately lead to the improvement of the security of the IoT.

TABLE I. SECURITY REQUIREMENTS IN THE FIELD OF IOT

Row	Requirement	Description	Category
1	confidentiality	Protection from unauthorized disclosure of information	Information flows
2	Integrity	Ensuring the correctness or correctness of the information	
3	Authentication	Ensuring that only authorized entities can access information	
4	Access level	Classification of access based on permissions	
5	non-denial	Ensuring that the sender or receiver does not deny sending or receiving information	
6	Privacy	Non-disclosure of sensitive information of people	social
7	Anonymity	The possibility of activity without the need to introduce the real identity	
8	Responsibility	Accepting the legal consequences of people's activities	
9	trust	Accepting people's approval	
10	Management of security keys	Including how to use public and private keys	encryption
11	Protocols	Guidelines and standards to be followed	
12	Security of hardware elements	Protection of hardware elements against various damages	Physical care
13	Embedded chip security	Protection against penetration and modification of embedded chips	

IV. IOT SECURITY MODELS

As shown in Fig. 1, in old information systems, there are three components of communication, control and calculation. There is a link between communication and control, which is sometimes called "information" and sometimes called "sensor network", which means collecting information from the control part and then putting it in the communication part. There is another link between communication and calculation, which is called "Internet" in China and "Cyber" in America [22, 29, 37].

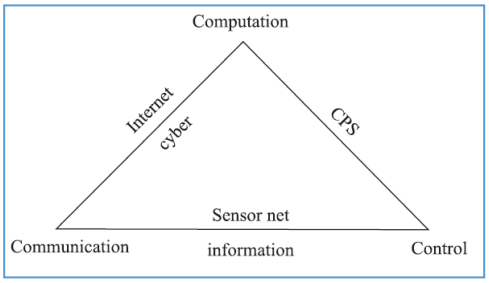

Fig. 1. IoT Model [22,34].

Theoretically, there is no link between control and calculation because control depends on the intervention of people. With the advent of the IoT, the link between control and calculation has also been established, which has made the impact of calculation results on control possible. This link, called CPS, is a real bridge connecting the data layer to the physical layer. In a broad sense, the entire diagram of Fig. 2 is the IoT, which includes cyber. But in a smaller sense, IoT refers to the link between computation and control. With the emergence of this link, it is expected to face a new security challenge called "direct control. Although the control should be done without human intervention, a security control should be used to prevent hackers from interfering. Therefore, considering this issue, the security model of the IoT according to Fig. 2 requires a security control between calculation and control [22, 33].

In Fig. 3, a model called U2IoT is presented, which is a heterogeneous system, including Unit IoT and Ubiquitous IoT. This model uses social factors for security layers and adds intelligence and adaptability to security requirements. At the core of this model, the IoT Unit is similar to the human neural network, which refers to a primitive cell that provides responses for specific applications. Ubiquitous IoT includes industrial, local, national and public Internet of Things, which is the result of the integration of several IoT Units and is similar to the social organization framework. Specifically, Unit IoT includes IoT networks, sensors, distributed control nodes, management and centralized data center (M&DC), and Ubiquitous IoT also includes industrial data center and management (iM&DC), local data center and management (lM&DC), and National Data and Management Center (nM&DC) [23, 30, 39].

Fig. 4 shows the security layers and requirements of the U2IoT model. In this figure, the x-axis is related to U2IoT, the y-axis is related to security requirements, and the z-axis is related to security layers.

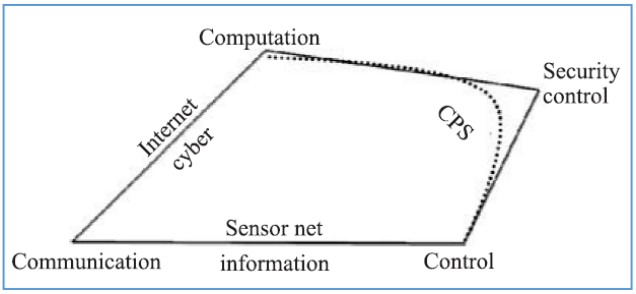

Fig. 2. IoT Security Model.

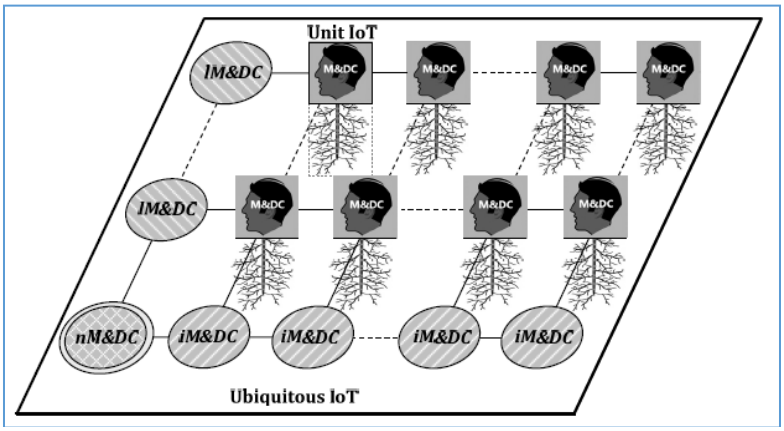

Fig. 3. U2IoT Security Model [23].

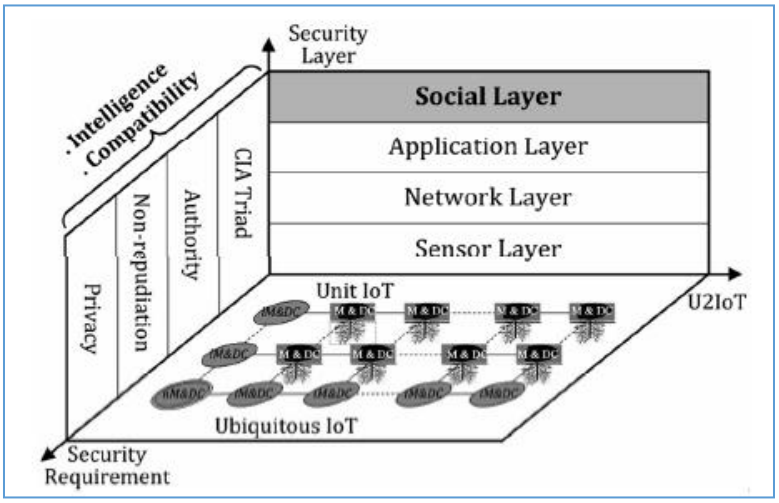

Fig. 4. Security Layers and Requirements of the U2IoT Model[23].

In this model, security is divided into four layers: sensor, network, application, and social. In the sensor layer, entities are observed to extract information and discover semantic resources. Also, special techniques are used to detect the effective Integrity and adaptation of imprecise information interactions. The network layer includes network interfaces, communication channels, network management, information storage, and intelligent processing. In this layer, centralized, distributed, and hybrid network topologies are used to help monitor and maintain the network configuration in real-time. In this layer, the safe transfer of information is ensured by using algorithms for coding, extracting, integrating, reconstructing, exploring and aggregating data. The main function of this layer is to transfer and process the information obtained from the sensor layer and realize data exchange between high-scale heterogeneous networks.

Application layer provides functionality for specific applications and provides implicit interfaces to the infrastructure to perform testing, monitoring, and auditing applications. Standard protocols and service composition technologies have been applied to realize integration between heterogeneous distributed networks and its applications such as support monitoring, intelligent scheduling, intelligent search, and cloud computing. Such applications must be adapted for dynamic environments. The social layer includes social features in the U2IoT model. This layer is basically provided for communication between objects and other support networks to establish correlation between cyber characteristics and its corresponding profile in social networks. Corresponding social characteristics are assigned to each entity and hierarchical management and data centers implement general security considerations. In the social layer, various interfaces are available to entities that act on their cyber existence and control their behavior. Meanwhile, in this layer, other social combinations are also considered, such as property control management, social relationship modeling, and entity behavior formulation. The security requirements considered in this model are three CIA (Confidentiality, Integrity and Availability), Authority, Non-repudiation, and Privacy, which bring reliable security along with privacy protection [23].

V. IoT Security Architectures

So far, various security architectures have been proposed for the IoT. The main difference between the presented architectures is related to the number of layers and also the difference in performance of each layer in the IoT architecture. Fig. 5 presents a four-layer architecture including sensing, network, support, and application layers. The sensory layer

collects all the information through the physical equipment and identifies the physical world. The information collected by this layer includes object characteristics, environmental conditions, etc. Physical equipment also includes all types of sensors, including GPS and RFID, which are responsible for collecting data and information. In fact, sensors are the key component of this layer that captures the physical world and displays it in the digital world. The network layer is responsible for the reliable transmission of information from the sensory layer, primary processing, classification and combination of information. In this layer, information transmission is based on several main networks, including the mobile Internet communication network and satellite networks. Also, network infrastructure and communication protocols are also required to exchange information between devices. The support layer establishes a platform for reliable support of the application layer. On this support platform, all intelligent computing capabilities will be organized through grid network and cloud computing. This layer plays the role of combining the application layer upwards and the network layer downwards. The application layer provides services such as personal information services, smart transfers, and environmental monitoring according to the needs of users. In fact, users will access the Internet of Things through application layer interfaces using televisions, personal computers, mobile devices, and the like. In the presented model, network security management is integrated with all the different layers of the architecture and manages them at different levels [24, 31, 32].

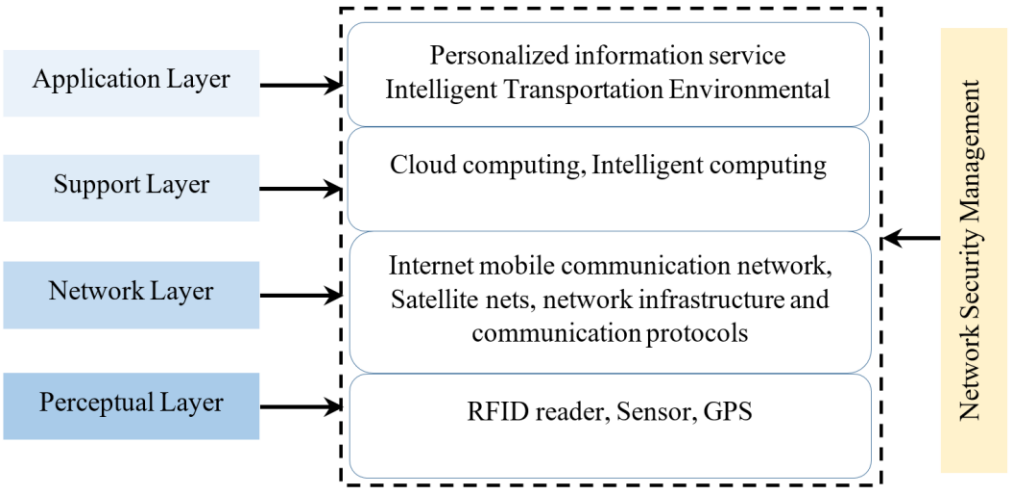

Fig. 5. Four-Layer Security Architecture of IoT [24].

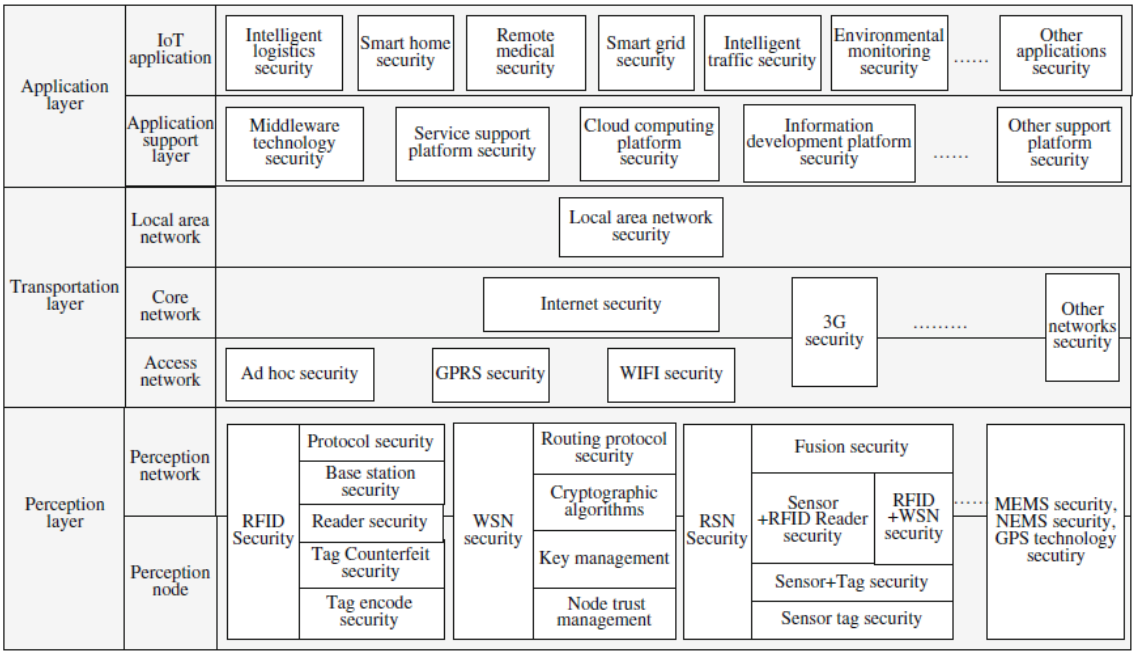

Fig. 6. Three-Layer Security Architecture of IoT[25].

Fig. 6 shows a three-layer architecture including the sensing layer, the transmission layer, and the application layer. This architecture has divided each layer into several sub-layers. The sensory layer is divided into two sublayers of sensory nodes and sensory network. The transmission layer is divided into three sublayers: access network, central network, and local network. The application layer is also divided into two application support sub-layers and Internet of Things applications. Each layer in this architecture has its own technical support. These technologies play an irreplaceable role at all levels. These techniques are more or less related to the range of existing issues that cause insecurity, privacy and other data security issues [25].

The IoT must ensure the security of all layers. In addition, the security of the Internet of Things should include the security of the entire system. The sensory layer includes RFID security, wireless sensor network security, RSN security, and anything else related to this layer. The transport layer includes access network security, central network security, and local network security. For example, 3G access network security, Ad-Hoc network security, WiFi security, and GPRS security are related to the access network substrate. Internet security is related to the security of the central network sublayer and local network security is related to the local network sublayer in the transmission layer. The application layer also includes application support and specific applications of the Internet of Things. Security in the support layer includes middleware technology security, service support platform security, cloud computing platform security, information development platform security, and other support platform; security must ensure the security of all layers. In addition, the security of the Internet of Things should include the security of the entire system. The sensory layer includes RFID security, wireless sensor network security, RSN security, and anything else related to this layer. The transport layer includes access network security, central network security, and local network security. For example, 3G access network security, Ad-Hoc network security, WiFi security, and GPRS security are related to the access network substrate. Internet security is related to the security of the central network sublayer and local network security is related to the local network sublayer in the transmission layer. The application layer also includes application support and specific applications of the Internet of Things. Security in the support layer includes middleware technology security, service support platform security, cloud computing platform security, information development platform security, and other support platform security. IoT applications in different industries have different application requirements. For example, smart home security requirements are different from telemedicine security requirements or smart traffic security requirements, and they should be specified according to the type of application of the relevant requirements [25].

Fig. 7 shows the security architecture in three layers of sense, network and application and middleware. In this form, middleware and application are considered in one layer. In the sense layer, hashing algorithms, encryption mechanisms, anonymity methods, risk assessment and intrusion detection are placed. In the network layer, peer-to-peer encryption, routing security, data integrity and intrusion detection are considered. In the application and middleware layer, integrated identity recognition, cryptographic mechanisms, firewalls, risk assessment, and intrusion detection are placed [26].

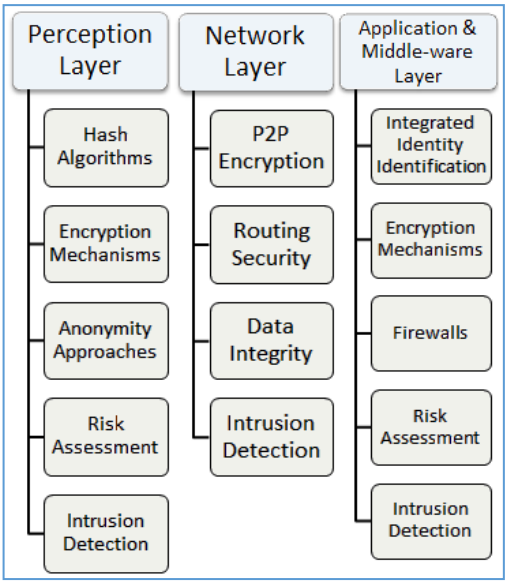

Fig. 7. IoT Security Architecture [26].

In Fig. 8, a security architecture for the U2IoT model is presented. In this architecture, three parts of information security, physical security and management security are considered. Information security covers security layer and security requirement. Physical security covers external content and core infrastructure, including intrinsic security and adaptive security. Security management includes application requirements, national/local/industry regulations, and international policy and standards. In this architecture, the connection of the U2IoT model with the security architecture at the cyber, physical and social levels is considered [38, 40].

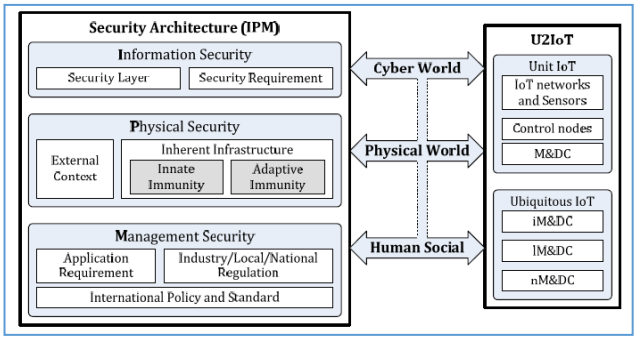

Fig. 8. Security Architecture of the U2IoT Model [23].

VI. The Proposed Framework for Managing Security in the Internet of Things

In order to create a comprehensive security in the Internet of Things, it is necessary to ensure the security of all the entities of the Internet of Things at different levels from different aspects. For this, it is necessary to first define the different entities of the Internet of Things. Generally, the following entities can be imagined in the Internet of Things:

- Objects: are the main components of the Internet of Things.
- Communication networks: networks that provide communication between objects.
- Internet: establishes the global connection of different communication networks.
- Users: a set of human agents who are the main users of the Internet of Things.
- Applications: Manage objects to meet users' needs.

A. Objects

There are different types of objects, and according to the type of each object, its security requirements will also be different. Generally, objects can be classified into three different categories based on how they interact with their surroundings:

- Sensor: They collect information from the surrounding environment. (example: camera).
- Stimulator: execute commands in their surroundings. (example: door lock).
- Combined: perform both sensor and actuator functions. (example: robot).

It is obvious that the security requirements of a sensor object that only collects information from its environment will have important differences with the security requirements of an actuator object that only executes commands in its environment, and a hybrid object must also meet the security requirements of two types benefited previously. For greater simplicity, a composite object that is both a sensor and a trigger is conceptually divided into two different parts, and security requirements can be entered for each part separately based on its functionality. Therefore, from now on, only the first two types will be considered. A sensor must be able to evaluate and validate the accuracy of its observations, and only if this evaluation and validation is correct, it can encrypt its observations using its private key and propagation the encrypted packet in the communication network for predefined purposes. With this, the requirements of comprehensiveness and confidentiality will be met. Fig. 9 shows the proposed model for sensor security in the Internet of Things.

According to Fig. 9, in the proposed model, two modules of physical care and intrusion detection are also used to increase the security of sensors. The physical guard module ensures the security of the hardware elements and chips embedded in the sensor, and the intrusion detection module is an intrusion detection system embedded in the sensor, which investigates the intrusion of hackers into the sensor. If a sensor has been compromised, it will be notified to other related departments using cryptography. By doing this, other entities can isolate the compromised sensor before any malicious action by the attacker and prevent any further damage. The use of cryptography in sensors has other advantages, for example, any suspicious activity can be reported. Therefore, a secret communication layer is created between different entities and the sensor, which makes other entities aware of the danger before any serious incident and before they succeed in attacking the sensor. All the entities that need the information of a sensor can decrypt the information sent by the sensor only if they have the public key of that sensor. In addition, the communication network is responsible for checking and authenticating entities that request to use sensor information. In fact, the communication network must guarantee that only authorized entities have access to sensor information. This is done through a predefined protocol. This protocol is defined by each application separately and exclusively. This will satisfy the authentication and access level requirements .The commands that are given to an actuator for execution must also be previously encrypted using special keys, and the actuator must also decrypt the commands using the key it has. In addition, a stimulus must be able to evaluate and verify the correctness of the commands it has received for execution, and only if this evaluation and verification is correct, it can execute the received commands in the external environment. Fig. 10 shows the proposed model for actuator security in the Internet of Things. In this model, as well as the proposed model for the security of sensors, the physical surveillance module and the intrusion detection module are used. Since an actuator, unlike a sensor, cannot send information to other entities, therefore, it cannot inform other entities of the dangers that have happened to it in a normal way, like a sensor. Therefore, an innovative method is used to inform other entities of dangerous conditions and intrusion into a trigger. In this method, a certain behavior is hidden in the execution of the commands of an actuator, and other entities, by observing this hidden behavior in the executive behavior of the actuator, will notice its critical condition and take the necessary measures to minimize possible damages. Although this idea adds a hardware overhead to the system, the resulting advantage is also significant. In other words, for each actuator, one or more sensors, which call monitoring sensors, are assigned to check the behavior of the stimulus, and in case of observing an abnormal behavior or a hidden behavior that is already defined in the intermediate protocol, the necessary notification done and the required security measures will be taken.

It should be noted here that all the explanations that were previously provided about how to manage keys and predefined protocols for sensors are now also true about how to manage keys and define protocols for operators, and repeating it is avoided.

B. Communication Networks

Communication networks are networks that establish communication between objects. In order to establish secure communication between objects, it is necessary to pay attention to logical communication in addition to physical communication. As an example, suppose that in a smart home there are security cameras and electronic alarms in a communication network. Now, is it reasonable that a security camera can issue commands that lead to the opening of the electronic lock on the door or not? Therefore, a communication network should be able to perform certain security controls based on a series of pre-defined protocols and policies, in addition to establishing the ability to exchange information between different objects and creating a secure communication channel. As mentioned earlier, these protocols and policies are

defined by the respective applications. Fig. 11 shows the proposed model for a communication network in the Internet of Things.

As can be seen, in this model, an anomaly detection module is used for network management. This module can detect anomalies based on communication channel activities, as well as pre-defined applications, protocols, and policies, and report them to the network management unit. The network management unit will also prevent unnecessary and suspicious communication if necessary. In this way, a double intelligence will be created in the communication network, which will ultimately improve the security of the Internet of Things.

C. Internet

The Internet, as the main infrastructure of the Internet of Things, establishes the global connection of various communication networks. In this way, access to objects from anywhere in the world will be possible. This issue will make the requirement of accessibility, which is one of the main requirements of the Internet of Things, be met. Since the communication of objects in the proposed model has a hierarchical structure, therefore, in the proposed model, there is a very good savings in assigning unique identifiers to objects. In other words, a unique local identifier is assigned to each object in the respective communication network, and a unique global identifier is assigned to each communication network. In this way, by using the sum of two network identifiers and the object, a global unique identifier will be obtained, which makes the addressing of each object unique in the world. In addition, more hierarchical levels can be used for this purpose. In this way, a suitable answer will be created for one of the basic challenges of the Internet of Things, which is related to assigning a unique identifier to each object.

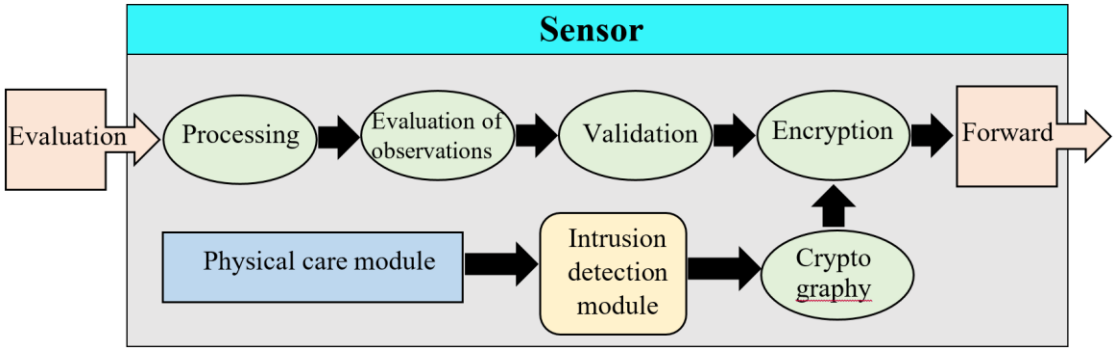

Fig. 9. Proposed Model for the Security of Sensors in the Internet of Things.

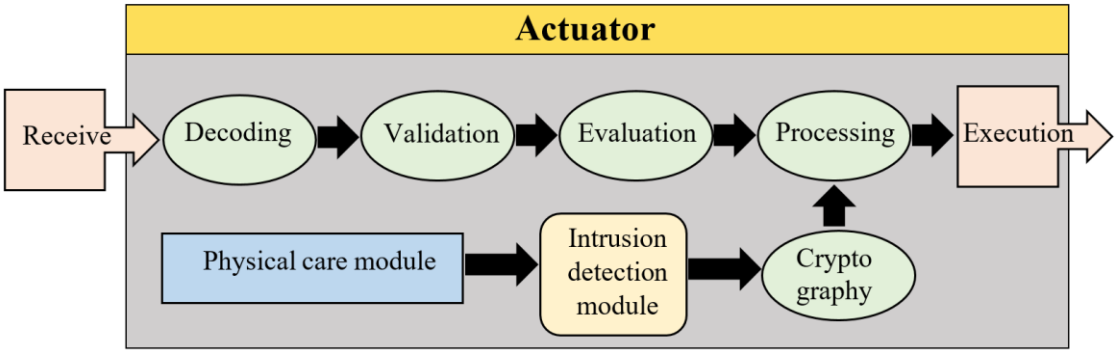

Fig. 10. Proposed Model for the Security of Actuator in the IoT.

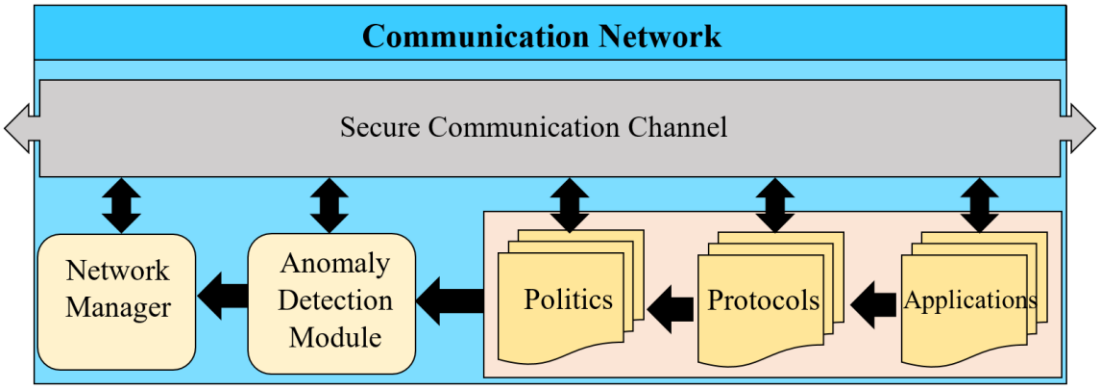

Fig. 11. Proposed Model for Communication Network in IoT.

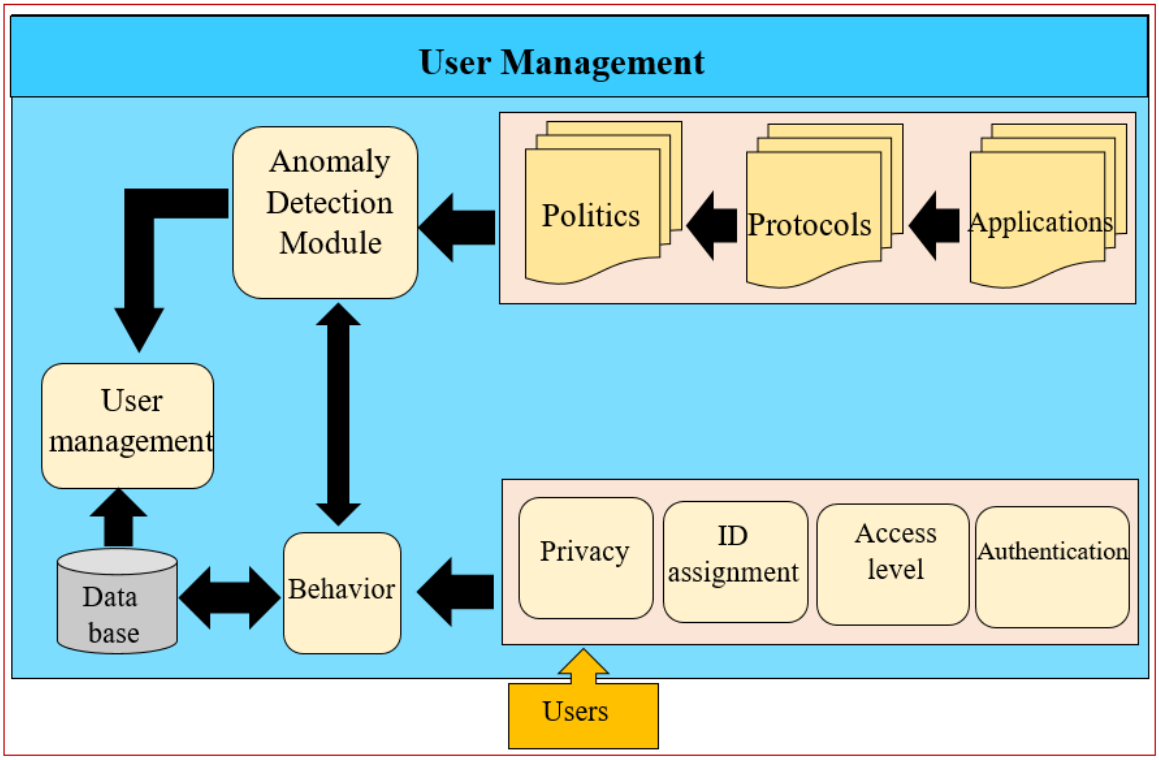

Fig. 12. Proposed Model for Managing Users in the IoT.

D. Users

Users are a set of human agents who use the Internet of Things to perform their desired applications. Generally, users can be divided into three different categories:

- Users: there are people who only use the Internet of Things at the user level.
- Managers: There are people who define applications and protocols at the management level.
- Attackers: unauthorized people who put themselves in the place of one of the above two groups and implement their goals.

User management is one of the most sensitive activities that must be done in the Internet of Things. In this regard, there are many security requirements such as authentication, access level determination, privacy, anonymity, responsibility and trust that must be covered. Fig. 12 shows the proposed model for user management. In this form, the components of authentication, access level determination, ID assignment, and privacy work in parallel, and an additional component called "behavior check" examines the behavior of users and stores the necessary information in the behavior database. This information is used along with applications, protocols and policies to detect anomalies in user behavior.

As shown in the Fig.12, the main idea in the proposed model is to use the behavioral characteristics of users to detect anomalies, and finally, by using the obtained information as well as the information in the database, user management operations are performed. This operation can include activating or deactivating users as well as issuing or not issuing access licenses for them.

E. Applications

Applications are responsible for managing objects to meet the needs of users. In fact, applications determine how objects should be related to each other and what mission they should perform. Applications also determine what activities different users can perform in the Internet of Things. In fact, applications provide a set of protocols, each of which provides a set of policies that are used in all the models described so far. As an example, consider the application of a smart air conditioning system.

In this application, the temperature and humidity sensors as well as the electronic key actuators of the cooling and heating system are defined as endpoints. The final task of this application is to adjust the temperature of the environment based on the needs of the users. Therefore, it is necessary for users to be able to determine the optimal minimum and maximum temperature. With this explanation, this particular application provides a set of protocols that describe how sensors, actuators, and users communicate. In addition, each of these protocols also provides a set of policies. For example, setting the minimum temperature by the user leads to a protocol that shows how the user interacts with the relevant data and changes it. For this purpose, a set of policies is considered. As an example, assume a policy where the user is allowed to change only one temperature data grade per step. In fact, this policy ensures that there are no drastic changes in sensitive data at once. In addition, such a policy also provides the ability to observe and track user behavior. Fig. 13 shows how applications, protocols and policies interact.

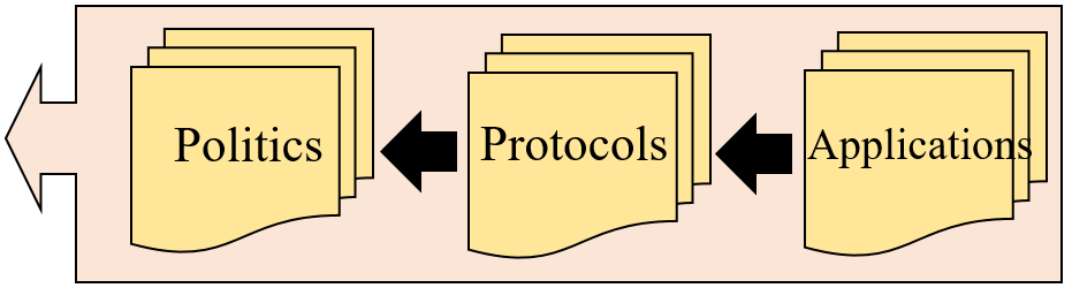

Fig. 13. Proposed Model for the Interaction of Applications, Protocols and Policies in the IoT.

VII. Evalution and Results

To evaluate the proposed method, after simulation, various scenarios are executed and the success or failure of the system in detecting and responding to an attack is measured as a measure of accuracy. Of course, to create diversity in the tests, a random number has been used, which generates identifiers for the objects that are the target of the attack, and the desired scenario is executed on it.

Also, to achieve stable and reliable results, according to the number of sensors and actuators, each experiment with random object ID is repeated 100 times and the average accuracy obtained is shown.

As can be seen from the above graphs (Fig. 14 and Fig.15), in general, the accuracy of the proposed method is significant. The point that should be noted here is that based on the tests, the proposed method is completely (100%) resistant against data modification attacks. It also performs well against impersonation attacks (97%). But against denial of service attacks, it has a lower detection accuracy (89%). This issue also seems quite logical because one of the prominent features of the proposed method is the use of behavioral and cryptographic parameters, which makes the resistance of the proposed method against change and impersonation attacks much higher than other attacks.

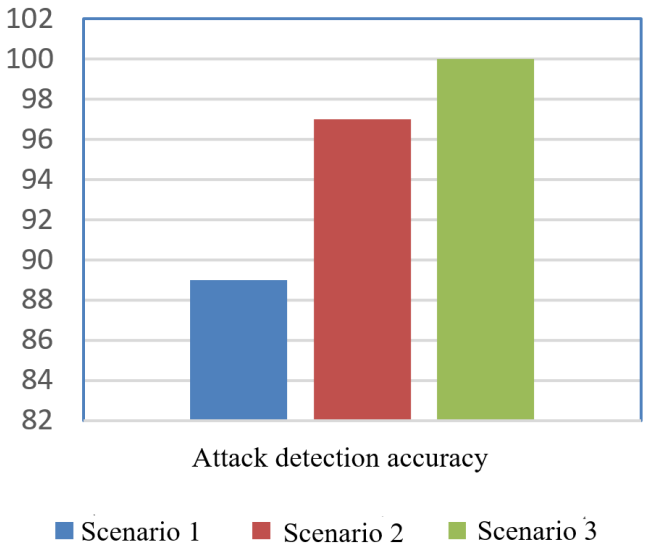

Fig. 14. Comparing the attack Detection Accuracy in Different Scenarios by Implementing the Proposed Method.

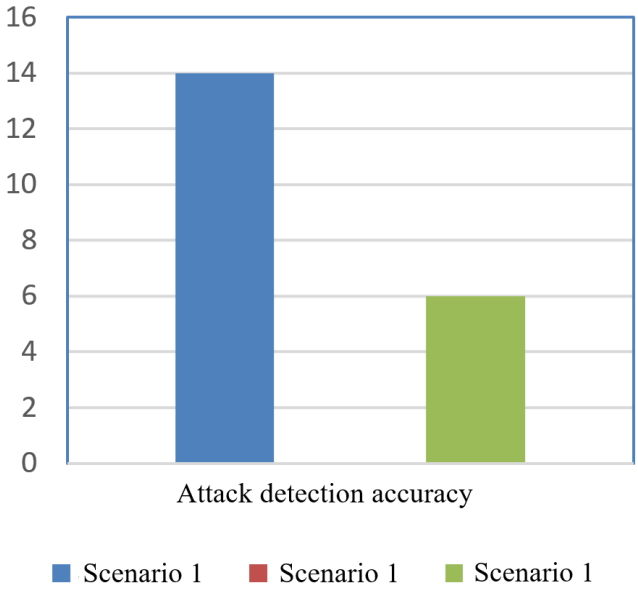

Fig. 15. Comparison of attack Detection Accuracy in Different Scenarios without Implementing the Proposed Method.

Contrary to this issue, if the proposed method is not used and relies only on the application and the centralized control system, the accuracy of attack detection will also be greatly reduced. In this case, the accuracy of detecting denial of service attacks is higher than others (14%), followed by the accuracy of detecting modified attacks (6%) and finally impersonation attacks cannot be detected at all (0%). It should be noted that these results are completely logical considering the way the mentioned system is implemented and its lack of use of impersonation detection mechanisms. Table II compares the mentioned results numerically.

TABLE II. Numerical Comparison of Test Results

Scenario	Attack detection accuracy without implementing the proposed method	Attack detection accuracy by implementing the proposed method
1	14%	89%
2	0%	97%
3	6%	100%

VIII. Conclusion

Until now, various activities have been carried out in line with the existing security challenges for the Internet of Things, but a comprehensive and integrated solution has not been provided for it, and more research is needed in this field. The

main activities carried out in the field of Internet of Things security are related to determining security requirements and providing models and security architecture. Generally, the security requirements in the field of Internet of Things can be placed in different categories, including data and information flows, encryption, social and physical care. Generally, the security models and architectures presented for the Internet of Things consider different levels and apply security issues at different levels separately. Therefore, there is a need to develop new models and architectures that cover all the security aspects of the Internet of Things in an integrated manner. For this purpose, the security requirements of the Internet of Things should be paid attention to from various aspects, and the connection between different levels should be fully seen in the security model of the Internet of Things. Although such work requires multiple activities and an optimal answer cannot be achieved at once. In this Paper, a new framework for managing security in the Internet of Things has been presented, which has presented solutions to improve security in the Internet of Things in a hierarchical manner and at different levels. The main focus of this framework has been relying on solutions for anomaly detection as well as intrusion detection, and in this regard, behavioral characteristics have been used, as well as data encryption of sensors and behavioral activities of actuator. What is specifically paid attention to in this Paper is the issue of notifying other departments by using encryption of the correctness of the operation or the possibility of detection of intrusion into the sensors and actuators, and based on the anomalies reported at the levels of the communication network and also manage users to make the necessary decisions. In other words, in the proposed model, the communication network is in charge of managing the network and it does this by using the protocols and policies specified by the applications and based on the observed anomalies. The user management level also uses the behavioral characteristics of users to detect anomalies and takes the necessary decisions if abnormal behaviors are observed. In other words, at this level, by storing user behaviors, a behavioral database will be created, which will be the main basis for subsequent decisions. This database stores user behaviors like a long-term memory and can be used in various ways. For example, this database can be used to track user activities and distinguish real users from attackers who intend to infiltrate the system.

REFERENCES

[1] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(3), 1622-1658.

[2] Shi, V. T., & Nhg, D. R. (2022). Channel Estimation Optimization Model in Internet of Things based on MIMO/OFDM with Deep Extended Kalman Filter. *Advances in Engineering and Intelligence Systems*, *1*(02).

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

[4] Thilakarathne, N. N., Kagita, M. K., & Priyashan, W. D. (2022). Green internet of things: The next generation energy efficient internet of things. In Applied Information Processing Systems (pp. 391-402). Springer, Singapore.

[5] Azad, F. A., Rad, S. A., & Arashpour, M. (2022). Back-stepping control of delta parallel robots with smart dynamic model selection for construction applications. Automation in Construction, 137, 104211.

[6] Mozaffari, H., & Houmansadr, A. (2020, January). Heterogeneous private information retrieval. In Network and Distributed Systems Security (NDSS) Symposium 2020.

[7] Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for internet of things. Sensors, 21(3), 772.

[8] Balachandar, S., & Chinnaiyan, R. (2019). Centralized reliability and security management of data in internet of things (IoT) with rule builder. In *International Conference on Computer Networks and Communication Technologies* (pp. 193-201). Springer, Singapore.

[9] Huang, X., Craig, P., Lin, H., & Yan, Z. (2016). SecIoT: a security framework for the Internet of Things. *Security and communication networks*, *9*(16), 3083-3094.

[10] Paniagua, C., & Delsing, J. (2020). Industrial frameworks for internet of things: A survey. *IEEE Systems Journal*, *15*(1), 1149-1159.

[11] Hosseini, S., & Khamesee, M. B. (2021). Modeling And Simulation And Imaging Of Blood Flow In The Human Body. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 13235-13244.

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

[13] Tan, L., Shi, N., Yu, K., Aloqaily, M., & Jararweh, Y. (2021). A blockchain-empowered access control framework for smart devices in green internet of things. *ACM Transactions on Internet Technology (TOIT)*, *21*(3), 1-20.

[14] Zhang, J. (2021). Distributed network security framework of energy internet based on internet of things. *Sustainable Energy Technologies and Assessments*, *44*, 101051.

[15] Ali, A., Mateen, A., Hanan, A., & Amin, F. (2022). Advanced Security Framework for Internet of Things (IoT). *Technologies*, *10*(3), 60.

[16] Panneerselvam, N., & Krithiga, S. (2022). A novel security framework for densely populated Internet of Things users in pervasive service access. *Computer Communications*, *184*, 86-95.

[17] Mutunhu, B., Chipangura, B., & Twinomurinzi, H. (2023). A Systematized Literature Review: Internet of Things (IoT) in the Remote Monitoring of Diabetes. In *Proceedings of Seventh International Congress on Information and Communication Technology* (pp. 649-660). Springer, Singapore.

[18] Liu, Y., Alzahrani, I. R., Jaleel, R. A., & Al Sulaie, S. (2023). An efficient smart data mining framework based cloud internet of things for developing artificial intelligence of marketing information analysis. *Information Processing & Management*, *60*(1), 103121.

[19] Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer Law & Security Review, 26(1), 23-30.

[20] Mozaffari, H., Houmansadr, A., & Venkataramani, A. (2019, December). Blocking-Resilient Communications in Information-Centric Networks using Router Redirection. In 2019 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[21] Chandrashekhar, A. M., Chaitra, K. V., & Koti, S. (2016). Security Fundamentals in Internet of Things. International Journal of Research, 3(01), 854-860.

[22] Granjal, J., Monteiro, E., & SaSilva, J. (2015). Security for the internet of things: a survey of existing protocols and open research issues.Communications Surveys & Tutorials, IEEE, 17(3), 1294-1312.

[23] Aufner, P. (2020). The IoT security gap: a look down into the valley between threat models and their implementation. International Journal of Information Security, 19(1), 3-14.

[24] Azimirad, V., Sotubadi, S. V., & Nasirlou, A. (2021, November). Vision-based Learning: a novel machine learning method based on convolutional neural networks and spiking neural networks. In *2021 9th RSI International Conference on Robotics and Mechatronics (ICRoM)* (pp. 192-197). IEEE.

[25] Wang, B., Liu, X., & Zhang, Y. (2022). Internet of things. In Internet of Things and BDS Application (pp. 71-127). Springer, Singapore.

[26] Ning, H., & Liu, H. (2012). Cyber-physical-social based security architecture for future internet of things. Advances in Internet of Things, 2(01), 1.

[27] Radhoush, S., Bahramipanah, M., Nehrir, H., & Shahooei, Z. (2022). A Review on State Estimation Techniques in Active Distribution Networks: Existing Practices and Their Challenges. *Sustainability*, *14*(5), 2520.

[28] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

[29] Fortino, G., Guerrieri, A., Savaglio, C., & Spezzano, G. (2022). A Review of Internet of Things Platforms through the IoT-A Reference Architecture. In International Symposium on Intelligent and Distributed Computing (pp. 25-34). Springer, Cham.

[30] Trik, M., Molk, A. M. N. G., Ghasemi, F., & Pouryeganeh, P. (2022). A Hybrid Selection Strategy Based on Traffic Analysis for Improving Performance in Networks on Chip. *Journal of Sensors*, *2022*.

[31] Mohamed, A. M. A., & Hamad, Y. A. M. (2020, September). IoT security: review and future directions for protection models. In 2020 International Conference on Computing and Information Technology (ICCIT-1441) (pp. 1-4). IEEE.

[32] Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: challenges and solutions. Wireless Personal Communications, 119(3), 2603-2637.

[33] Yao, X., Farha, F., Li, R., Psychoula, I., Chen, L., & Ning, H. (2021). Security and privacy issues of physical objects in the IoT: Challenges and opportunities. Digital Communications and Networks, 7(3), 373-384.

[34] Trik, Mohammad, Amir Massoud Bidgoli, Hossein Vashani, and Saadat Pour Mozaffari. "A new adaptive selection strategy for reducing latency in networks on chip." *Integration* (2022).

[35] Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. SN Applied Sciences, 3(1), 1-14.

[36] Vahidi Farashah, M., Etebarian, A., Azmi, R., & Ebrahimzadeh Dastjerdi, R. (2021). An analytics model for TelecoVAS customers' basket clustering using ensemble learning approach. *Journal of Big Data*, *8*(1), 1-24.

[37] Trik, M., Mozaffari, S. P., & Bidgoli, A. M. (2021). Providing an adaptive routing along with a hybrid selection strategy to increase efficiency in NoC-based neuromorphic systems. *Computational Intelligence and Neuroscience*, *2021*.

[38] Ali, A., Mateen, A., Hanan, A., & Amin, F. (2022). Advanced Security Framework for Internet of Things (IoT). Technologies 2022, 10, 60.

[39] Mozaffari, H., & Houmansadr, A. (2022). E2FL: Equal and Equitable Federated Learning. *arXiv preprint arXiv:2205.10454*.

[40] Sun, J., Zhang, Y., & Trik, M. (2022). PBPHS: A Profile-Based Predictive Handover Strategy for 5G Networks. *Cybernetics and Systems*, 1-22.