A Proposed Model of IoT Security Management System Based on A study of Internet of Things (IoT) Security

Samah Osama M. Kamel[1], Nadia H. Hegazi[2]
Electronics Research Institute, Giza, Egypt[1, 2]

Abstract— The Internet of things (IoT) is a new intelligent communications in the world which provides many applications such as industry, communications, agriculture, business and etc. All researches and many organizations concentrate on the development of IoT to present many services and develop our life. The new technology faces many challenges such as architecture, standard and security. In this paper, we provide a thorough overview on the introduction of IoT including history, components, connection and application of IoT. IoT layers architecture has been explained briefly. We also discuss the IoT security and privacy challenges to solve most of IoT security problems, put rules and terms of services and achieve security requirements. The security requirements are the main part of designing the security solutions and IoT network management systems. Moreover, this paper presents a comprehensive background on the types and targets of attacks to recognize the internal and external attacks to prevent them. This study depends on the explanation of the categories of attacks and problems in each IoT security layer to introduce many security measures. The vision of this study provides the best selection of the convenient security mechanisms which provide low power consumption and time. This paper presents a proposed model of the security management for IoT. The proposed model is used to choose the appropriate security mechanisms and protocols for IoT security layers. This proposed model contributes to enhance the performance of IoT network by selecting the suitable security mechanisms for IoT layers to decrease power and time consumption.

Index Terms— Internet of Things, Radio Frequency Identification Device (RFID), Wireless Sensor Network (WSN), IoT security layer, End to End Authentication and Key Management..

1 Introduction

Over the last few years, IoT is flourishing as a new tecnology in the world. It is an expectation that the future of the world will be changed by using IoT technology over coming years. The leap of new IoT technology will introduce a new world of services which will develop the quality of life. The infrastructure of IoT had been implemented to modify the form of communications between devices and human to exchange a huge amount of information. So IoT creates a new flexible world of communication between people and billions of devices.

IoT becames the criterion for many applications especially, industry and communications. Moreover, IoT contributes to many fields such as agriculture, environment, medical sector, education, transportation, economic and etc. These applications present many major projects of IoT such as smart homes, smart transportations, smart factories, smart homes, smart farms, smart grids, smart hospitals, smart schools, smart city and etc. This new technology enhances and improves our daily life.

IoT has an important influence in the business sector where IoT market achieved profits that are 290 billion dollars in 2017. This profit will increase by 30 % per year. Moreover, IoT plays a significant role for people with disabilities and the elderly with many levels of independence at a reasonable cost.

It's obvious that the purpose of IoT creates the connection of computing devices, mechanical and digital machines, objects and people through applications using the web interface and mobile applications. The IoT environment has the capability of transferring data over the network without requiring human-to-human or human-to-computer communications. The IoT system has four main components which are categorized into things, communications, applications and data analysis.

The IoT technology takes advantages of every object and creates a new system with new capabilities.

IoT has a large number of smart objects and this number will increase to 50 billion objects by year 2020 [44]. There are many companies and scientific research organizations introduce a practical blueprint for IoT impacts on the economy and most of the life fields over the ten years. Cisco is the first company that presents many projects which encompass more than 24 billion smart objects by 2019. Moreover, Morgan Stanley company envelopes many projects with billions of smart objects and this number will be increased to 75 billion connected devices by 2020. All expectation refers to that Huawei Company will present 100 billion IoT connections by 2025 [17, 19, 27]. It is obvious that there is strict competition among most of the companies to present IoT network with numerous billion of connected smart objects.

This introductory section provides a brief overview of the IoT history. In 1982, the idea of the internet initiated using Internet Protocol (TCP/IP). The idea of the interconnection of many devices was crystallized to create the Internet term [15]. In 1990, John Romkey and Simon Hackett created a toaster which was connected to the Internet using TCP/IP protocol and was controlled by using a Simple Networking Management Protocol Management Information Base (SNMP MIB) [14]. The term of the IoT initiated when Kevin Ashton coined the concept of the Internet of things IoT and established MIT's Auto-ID Center in 1999. His idea focused on linking RFID information to the Internet. This idea was simple and robust which provided the connections between all devices and each other [31]. In1999, Andy Stanford-Clark of IBM and Arlen Nipper of Arcom (now Eurotech) created a machine to machine protocol which was the first protocol for connecting devices called MQ Telemetry Transport (MQTT) [78]. In 2000, LG Company announced the first connected refrigerator. The idea of the connected refrigerator was built using barcode and RFID scanning [23]. In 2008, the IPSO Alliance promoted Internet Protocol connections through smart objects. IPSO Smart Objects was a project which provided a connection between smart objects and software applications of other devices and services [29]. In 2010, Google Company introduced a project called a self-driving vehicle. This project converted the traditional control into intelligent control by developing a connected and autonomous car. This car included a sensor and camera which are hanged on top of a Toyota Prius. The project was considered a new invention in industry and communications technology [69]. In 2010, many types of research started to solve problems of IoT such as Bluetooth and high power consumption. These researches presented a new technique to introduce smart Bluetooth called Bluetooth Low Energy (BLE). BLE provides many applications in the fitness, healthcare, security, and home entertainment industries [47]. In 2013, IoT uses many technologies such as wireless communication, micro electro mechanical system (MEMS) and embedded systems to produce many technologies and applications [15].

From the previous sections, it is clear that the nature of IoT is heterogeneous network which contains billion of different smart objects or things (devices). The smart objects or things can be physical and virtual. Physical things are sensors and electrical objects while virtual things are information or data which is collected, preprocessed, stored and accessed.

There are three connections to transfer data which are categorized into the machine to machine (M2M), machine to human (M2H) and human to human (H2H) connections [38].

But it is important to ask what the differences between IoT and the Internet are. The features of IoT will be discussed in the forthcoming sections. These features reflect the characteristics of IoT. To better understand the characteristics of IoT, it should clarify some fundamentals characteristics of IoT such as heterogeneity, dynamic changes, enormous scale and interconnectivity. With regard to heterogeneity, there is a large number of different devices in IoT with different hardware and software platforms. These devices can interact with each other through different networks [38]. So the operations among different devices are very complex. For this reason, the security systems of IoT are weak mechanisms to face many threats and attacks. With respect to dynamic changes, IoT should provide a dynamic environment to detect any change in devices state without requiring to deal with human or devices. The changes of devices can be seen in many forms such as sleeping, waking up, connected or disconnected. Moreover, the location and speed of the devices are altered automatically [38]. As a result of this, there are authentication, authorization and access control problems. In this moment attackers can exploit easily these problems to gain access, monitor and destroy data and devices themselves.

In the case of enormous scale, every device in IoT generates data so IoT devices produce a huge amount of data. A huge amount of data needs to be analyzed and processed. Thus many of services require management of big data analysis. Moreover, all devices should be managed and communicated with each other.

In terms of interconnectivity, any device can connect and communicate to the Internet. The interconnect features provide network accessibility and compatibility.

New device or human can integrate with IoT devices using an authentication mechanism. IoT system can provide automatic identification process for new device or human. All features of IoT provide integration, control, indexing, tracking, connectivity and autonomous operations.

The features of IoT revealed the advantages and disadvantages of IoT. The advantages of IoT can be summarized as the following section.

IoT converts the traditional control to the intelligent control. Therefore IoT can improve the intelligent of interconnection between physical and virtual objects to create a new remote control system. The intelligent control provides that all smart objects control automatically a large amount of data. The intelligent control is used to save time.

IoT provides accurate data through offline and online analysis. This process contributes to decision making and puts the end of all problems of data collection. IoT can provide efficiency and low operating costs by using many means such as improving utilization, process efficiencies and productivity such as smart meters. Smart meters eliminate manual meter readings which leads to decline billions of dollars.

However, IoT system has a number of serious drawbacks. Complexity is the most significant problem because IoT operations are very complex and there is no flexible integration among devices. There are different devices with different design, deployment and maintenance so any weakness in software or hardware will have serious problems [71]. IoT network suffers from authentication and access control problems because smart objects are heterogeneous devices which are based on different platform (hardware and networks). Moreover, all devices need to interact with other devices through different networks. Thus, security problems are the biggest challenge because all devices and data are exposed to all kinds of threats and attacks. There are different threats and attacks which may cause serious disasters in the network. Furthermore, all personal data of all users are exposed to the most dangerous attacks. In addition to, IoT hasn't regulations and rules to explain that how to secure devices and data.

This paper presents a proposed model which is used to build security management system for the IoT network to provide suitable security mechanisms for the IoT security layers. It can help designer to decrease time and power consumption.

The organization of this work will be as follows: Section 2 describes the challenges of IoT to identify and solve the IoT obstacles. Section 3 focuses on the security requirements to improve the performance of the IoT network. Section 4 discusses the definitions of threats, attacks, exposure and vulnerabilities. Section 5 describes IoT layers architecture and IoT security features. Section 6 displays the IoT security layers and their attack, problems and security measures. This section discusses the comparisons among the security measures and mechanisms in each layer. Section 7 presents the proposed model of the security management for the IoT network. The conclusion is presented in the final section.

2 IoT Challenges

IoT introduces many services and applications but IoT requires essential common protocol, techniques, architecture, standard and security mechanisms to achieve the integration between the virtual world and the real world in one platform. Generally, there are three IoT challenges which can be categorized into architecture, standard and security and privacy challenges. Regarding architecture challenge, as mention above, smart objects are increasing every day. Every different smart device generates data to provide many services anytime and anywhere. These services require infrastructure to support, integrate and analyze the generated data to predict the future decision. Therefore, IoT needs dynamic architecture to introduce an entire blueprint which is used for supporting different objects and applications [11].

With respect to standard challenge, IoT standard doesn't give adequate opportunity for objects to use and access network resource equally. Unfortunately, the traditional network standards aren't enough to support new smart objects and applications. So the IoT network should have a specific standard to support new object and application [11].

As mention above, IoT contains many sensors which have limited power. Thus the usage of the traditional security methods will not support IoT machine to machine connections. For this reason, IoT needs security mechanisms to achieve low computational power and convenient security systems. Attackers may use different techniques in different layers to destory the IoT network. So data security has become the priority consideration for the IoT network design. From this point, the IoT security and privacy challenges play a substantial role in the IoT system.

IoT security and privacy challenges can be illustrated in the following points:

1. User Privacy and Data Protection

The IoT system is based on conveying and exchanging information/data through mediums among diverse smart objects. The exchanged data may include personal information about users which reflects the personality and behavior of users. As mention above, the IoT system provides an automatic identification for any device and human. All information about users can be collected from their related objects which are stored in the system or transferred through mediums among diverse smart objects [31]. All private information of users without any authentication mechanisms are exposed to the most dangerous of attacks and threats. So the privacy and data protection play vital role in the IoT network.

Privacy is based on three main parts. First, secrecy is securing all messages which can only be understood by intended recipients. Second, anonymity is the ability to send and receive messages without revealing identity of the sender and receiver. Third, autonomy is avoidance of facing attackers.

2. Trust Management and Policy Integration

As the result of limited protocols, resources and capacity of different smart objects, there is an extremely big challenge of IoT trust management. Trust management is an important part of IoT security, information security, services, applications and user privacy. Trust management is an essential element of interactions among smart objects to exchange and manage data. IoT layers have different and heterogeneity devices. For example; each device generates a huge amount of data which are exposed to different attacks, threats and errors. These errors and attacks may be propagated in all IoT layers. So the accuracy of data and services quality will be decreased and users will not accept it. Trust management in IoT should achieve the following goals. First; it should provide trust relationships of the IoT objects and trust decision to communicate and cooperate with each other. Second; it should conserve user privacy, data transmission and trust communication according to policy integration of IoT. Third; it should increase the quality of IoT services, system security and robustness [83].

3. End-To-End Security

IoT contains billions of smart objects and each smart object sends a huge amount of data to other objects. A smart object should be authenticated and has security mechanisms to secure users, devices, and services. In the same time, security mechanisms are used to prevent threats and attacks to access data or services. This operation called End-to-End security. The domain of End-to-End security includes IoT devices, IoT gateway, access and network connectivity, IoT application, platform and users. The main requirements of End-to-End security are authentication, access control and encryption processes. The scenario of End-to-End security can be described briefly in view steps. When any smart object wants to connect to another one, both of them should be authenticated objects. Once a smart object is authenticated, it can send and receive data or commands. Then a smart object can directly connect to cloud. The responsible of cloud provides authentication process and controls messages among smart objects. After authentication and control processes are implemented, a smart object connects to the Internet through the gateway. Then the encryption process is used to encrypt messages which are exchanged among smart objects [82].

4. Authentication and Identity Management

Authentication mechanism plays an important role in IoT security and it can be implemented by many methods such as ID, password and public key infrastructure (PKI). But Traditional authentication mechanisms are not applicable for IoT because of objects heterogeneity and complexity [40]. Regarding identity management, it is used to manage identities, services and functions of smart objects. It provides identification, authentication and access control services. Identity management is used to define the connections of smart objects. It includes connectivity, network domains and applications in the IoT platform. Therefore, identity management depends on the strength of authentication mechanisms [37].

5. Authorization and Access Control

Authorization and access control mechanisms provide users to gain access to network resources and services. Authentication and access control prevent unauthorized users from gaining access to network resources. As mentioned above, IoT devices have limited storage capacity and power so the implementation of authorization and access control methodologies are not easy missions. In addition to the heterogeneity and complexity of devices, authorization and access control methodologies may be not applicable for IoT system [40].

6. Security Solutions and Threats Resistance

The security management system is used to identify the security methodologies of the IoT layers. It is used to prevent many attacks and threats. Security system strategy depends on protection of devices, transmission mediums, exchanged data, services and business models. The security solutions provide convenient environment for the IoT system to be suitable for the nature of different devices and applications. There are many security mechanisms such as Internet Protocol Security (IPsec), asymmetric and symmetric cryptography, authentication, etc. [67].

More broadly, it is also needed to determine the principles of IoT Security which are described briefly as follows. The main problem of IoT is that there are no rules, laws and terms of service to provide different levels of data protection. Therefore, the main principle is to set rules and laws and the companies and organization have the ability to use the IoT network in secure way.

The next principle is providing trusted web interface and mobile applications to facilitate the communications between people and smart objects through these applications. Moreover, mathematical algorithms are important issues for the implementation of IoT security methodologies like authentication and encryption processes. These mechanisms should be appropriate for different devices and applications.

3 Security Requirements

The security requirements become an essential part of the implementation of the efficient IoT. The design of security solutions and management system relies on the security principles. There are main requirements to achieve the IoT security system which are explained as follows [26, 51, 61, 55, 45].

- Availability

The goal of availability is to provide the ability of users to access services anytime and anywhere. It is important to conserve the connectivity between users and network resources all the time. Thus all users should be authenticated to fight attacks and threats to network resources. Availability may prevent bottleneck situations such as system conflictions and network congestion which have influence on data flow.

- Accountability

Accountability can't prevent attacks and threats in IoT but it is important to conserve and support the other security requirements such as integrity and confidentiality. It is used to trace any device which sends and receives data to observe and detect any unknown operations by providing regulations of devices, users and their actions or behavior.

- Auditing

Auditing is a vital principle of the security requirements to identify the security weakness of IoT. It is based on the evaluation system and services. It is used to measures that how IoT system matches to a specific standard of applications.

- Authentication and Authorization

The authentication is the most significant security requirement which identifies user as an authenticated object using security mechanisms such as public and private key (cryptography algorithms). In terms of authorization, it is used to give users permission to use network services or resources.

- Access control

Access control is implemented by network administrator to give users specific missions or authenticated access to use network resources such as reading, writing and editing or modification data. So access control provides authenticated users to implement specific tasks.

- Privacy

Privacy is used to insure the private information of users. It may prevent illegal users. There are many levels and forms of privacy such as:

1. Privacy in devices, it depends on physical and commutation privacy. Devices may be exposed to information theft.
2. Privacy during communication, it depends on the communications of IoT devices. It is used to prevent data disclosure during communication.
3. Privacy in processing and storage phases, it is used to protect the processed data.
4. Identity and location privacy, it is used to give a permission to authorized users to access the geographical position of IoT devices.

- Confidentiality

Confidentiality is an essential concept of security requirements to prevent unauthorized users to access data. Confidentiality provides identification, authentication and authorization for any smart object in the IoT network. There are many security mechanisms to guarantee the confidentiality of data such as authentication mechanisms.

- Integrity

Integrity is one of the security concepts which enables authorized users access, read, delete or modify data but under restricted conditions. So integrity can prevent internal attacks which is the most dangerous problem in the network because they are authenticated authorized users. In addition to, cybercriminals may change data during transmission so integrity may prevent external attacks to access or modify data.

- Non-repudiation

The meaning of non-repudiation can be easily explained. It is used to prove that the sender and receiver can't deny that their messages belong to them. So non-repudiation can prevent internal attacks.

4 Type of Threats, Attacks, Exposure, Vulnerabilities

This study shed light on the definitions of threats, vulnerabilities, exposure and attacks to provide the protection of the IoT system which is the most important topic for the time being. It considers the substantial part in the IoT security. Once the definition of attack is clear, it can be prevented. For example; some threats may damage physical devices, transmission mediums, mobile communication network, protocols, application servers, software, data storage or different services. The following sections articulate the definitions of threats and their goals.

4.1 Threats

Threats use the weak point of the IoT system security and damage or steal information. Threats may harm hardware and software. There are two types of threats which are classified into internal and external threats. Internal threats can be generated from the internal network. The internal attack is authenticated authorized users and they are the most dangerous threats. There are many goals of internal threats. First, threats can steal data and all information about biometrics identification system. Second, internal threats can exploit weakness of access control and damage authentication, authorization and accountability to control the access of users. This kind of threats can be prevented using a password or biometrics. Third, the reason of the power fluctuation is to the power surge which causes electronic equipment failure. This case can be solved using a surge protector.

External threats can be generated from unauthenticated user who uses codes and scripts to penetrate, control, or damage smart objects and steal data [51, 48]. External threats include virus, worm, Trojan and spyware. This kind of threats can be prevented using antivirus and antispyware.

4.2 Vulnerabilities

Vulnerabilities occur the network because of the weakness of system. This weakness permits attackers to access data, edit some commands or damage network by using Denial of Services (Dos) attack. It can be found in devices, operating system and application, communication protocol and network policies [51, 6]. There are many types of vulnerabilities such as virtual machine based rootkit, session hijacking, internet protocol vulnerabilities, byzantine failure and resource exhaustion. Regarding virtual machine based rootkit, it is a type of malware and works in the virtual environment (virtual operating system or application). It can be detected using strong security system for hardware and virtual machine. Regard to session hijacking, it refers to an attacker steals the session between two users to gain access to data to implement malicious activities. Man-in-the-Middle (MIM) attack is famous attack in cyber criminals. It exploits the weakness of internet protocols. This attack puts himself or herself between users and network to eavesdrop and capture data to modify, read or damage data. Regard as a Byzantine failure, it is a fault which occurs in cloud storage due to software bugs or hardware malfunction. It can be prevented by using cryptography algorithms. Resource exhaustion occurs due to consumption or leakage of resources and weak design. Finally, resource exhaustion causes DoS attacks [77].

4.3 Exposure

Exposure is a problem or mistake which occurs in system configuration. It leads to permit attackers to gain access to data. In this case, attackers may capture smart objects or get cryptographic keys. It can replace data or device with malicious one [51].

4.4 Attacks

The motivation of attacks is data and services theft or interception. So the targets of attacks are eavesdropping, access control and management of data and devices. The impact of attacks can be categorized into the passive attack and active attack. The mission of passive attack is only eavesdropping or gathering information about the network. It can be implemented using port scanning and Traffic analysis. It can't harm availability and integrity but harm confidentiality. The function of active attacks is modification, destruction and block information or resources. It harms confidentiality, availability and integrity.

There are two main entities of attacks that are internal and external attacks. Internal attacks are authenticated users in the network. They are the most dangerous type of attack because they destroy most of the security requirements. The external attackers are unauthenticated users which try to access the network using different ways.

The common types of attacks can be illustrated as follows:

- Physical-based attacks

This type of attack is named also device tampering. The scenario of this attack can be explained in the following section. All IoT devices are integrated with each other. In some time, some devices are unattended thus attacks can easily steal them and insert them into the network of attack. The target of this attack is to steal data, application manipulation or devices tampering [51, 5].

- Impersonation-based attacks

The scenario of this attack is illustrated as follows. When a user wants to talk another one, this user sends a login request message. The requested message contains the name and IP address of this user. An attacker can eavesdrop or intercept the requested message over the communication channel. At this moment, an attacker can impersonate authenticated user to modify all information [52].

- Data-based attacks

It is named as information disclosure or exposing. It means that database is exposed to unauthenticated users using data eavesdropping, session hijacking or illegal access to the device [51].

- Spoofing-based attacks

The target of the spoofing-based attack is to deceive network or users by breaking authentication mechanism. An attacker can deceive a user by making himself or herself as an authenticated user to steal data or communication. There are different types of spoofing which are categorized into IP spoofing and Address Resolution Protocol (ARP) spoofing. Regard to IP spoofing, an attacker can capture any message of user (Ex. e-mail). This message contains IP header. The attacker can change the IP header to appear that this message comes from authenticated user. Regarding ARP spoofing, an attacker can send forged address resolution protocol to link MAC of attacker of legitimate user. Once the IP address of attacker is connected to the true IP address, attacker can send and receive data to or from the network. There are many forms of spoofing attack such as MIM, DoS and session hijacking [70].

- Access-based attacks

Access-based attack occurs when an unauthorized user tries to gain access to the network. An attacker tries to connect to IP address and pretends as an authenticated user [51].

- Identity-based attacks

An attacker tries to steal the identity of device or user by using three steps. First, an attacker uses eavesdropping technique to listen to data. Second, an attacker uses tracking to trace of identification number of any user. Third, an attacker steals or duplicate password of users [51].

- Privacy-based attacks

Hackers can easily collect a huge amount of private information about users. There are many methods of privacy-based attacks. First, attackers can use malicious software to obtain secret information about users. Second, attackers can follow the location of users. Third, attackers can capture the password of users by cracking ways [51].

- Signal injection attacks

The meaning of signal injection attacks is that an attacker injects fake data into the network to gain access, change, and damage transmitted data [5].

- Side channel-based attacks

An intruder can find the encryption key and get access to data. There are many examples of side channel-based attack such as time analysis, power consumption, traffic analysis and private data [5].

- Sniffing or reconnaissance attacks

This type of attack sniffs any packet of network. Then it analyzes all information using port scanning, traffic analysis and packet sniffers.

- Denial of Service (DOS) attacks

It is the most dangerous attacks. The target of DoS is to flood the network with illegal requests to overload network and prevent all legal requests to access to the network. It causes consuming bandwidth and loss of network resources. It makes network services unavailable [39].

5 IoT Layers ARCHITECTURE AND IoT SECURITY FEATURES

5.1 IoT Layers Architecture

The IoT network consists of six layers, namely, coding, perception, network, middleware, application and business layers as shown in Figure 1.

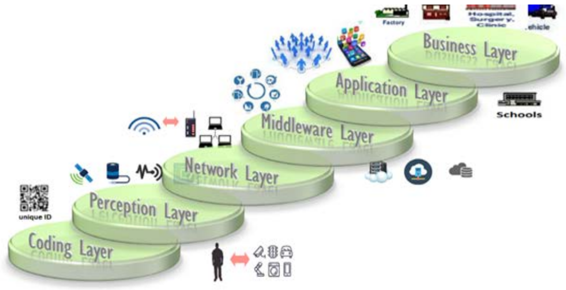


Fig. 1. IoT layers architecture

1. Coding Layer

Coding layer is the first layer of IoT and provides identification process for each smart devices IoT system. Each device is assigned a unique ID which distinguishes each device [44].

2. Perception Layer

The main equipment in the perception layer is Radio Frequency Identification Device (RFID), Wireless Sensor Network (WSN), all kinds of sensors, GPS, Bluetooth and etc. The main purpose of the perception layer is to link different devices in the IoT network. The basic functions of the perception layer are gathering data from different physical devices and conversion data into digital signal. Then the perception layer transmits data to the network layer [44, 56].

3. Network Layer

The main equipment of the network layer is mobile Communication network, Internet and any other kind of reliable network. This layer receives all information from the perception layer and transmits data to the middleware layer through transmission mediums such as Wi-Fi, Bluetooth, WiMAX, ZigBee, GSM, 3G, and 4G using communication protocols such as IPv4, IPv6, MQTT, and DDS. The network layer is responsible for processing, management and maintenance data [26].

4. Middleware Layer

The middleware layer receives a huge amount of information from the network layer and processes data using some intelligent processing systems such as cloud computing to provide direct access to database to store all information in cloud [45, 26]. The function of the middleware layer is based on Service Oriented Architecture (SOA) which consists of few processes that are grouped into applications, service composition, service management, object abstraction, trust, privacy and security management. The function of applications process is to take all functions of the system to final users. Service composition process gives functions to each smart object and manages them. Object abstraction process is responsible for the harmony access among different objects with common language. Trust, privacy and security management process is used to protect the exchanged data [42].

5. Application Layer

The application layer uses the processed data to achieve many of application. IoT applications are based on the requirements of the users such as industry, education, medical sector and communication so it is useful for IoT development [42]. The application layer uses different number of protocols, such as the constrained application protocol (CoAP), the message queue telemetry transport (MQTT) protocol, the advanced message queuing protocol (AMQP), and extensible messaging and presence protocol (XMPP).

6. Business Layer

The business layer is the final layer of IoT layers architecture. It is responsible for the management of applications and services of the IoT system. The business layer is used to generate different models which are used for different benefits [45, 56].

5.2. IoT security Features

The IoT security features reflect the IoT security characteristics which help us to put the tactical plan to face the problems of

IoT security. There are three traditional IoT security features and the remainder are modern features. The following section explained briefly each IoT security feature.

- Perception Layer Problems

As mention above, the main function of the perception layer is data collection and data transmission using sensor nodes which have limited power. The traditional security mechanisms are not convenient for the IoT system then the mission of designing of protection system is very difficult [36].

- Network Layer Problems

The network layer includes transmission data, mediums and protocols so there is diversity of different attacks in this layer. The security mechanisms of IoT should be strong to protect data, mediums and protocols [11, 36].

- Application Layer Problems

There are different applications in IoT. Then the IoT network is exposed to different attacks. This leads to leakage of data and access control problem.

- Identifying and Locating Objects

Identification methodology indicates the location of devices in the IoT system using Domain name system (DNS). DNS provides address mapping for each device and each device has name and IP address. This methodology is an insecure naming system because there are many attacks such as MIM and DNS cache poisoning attacks [40].

- Authentication and Authorization

As a result of heterogeneity and complexity of IoT nature, conventional authentication and authorization methods may not suitable for the IoT security system [33]. There are many researches to solve this problem.

- The contradiction between security and cost

There is contraction between security and cost. When IoT security level will be increased, the performance of nodes will be increased. So the cost of the network maintenance will be increased [36].

Lightweight security algorithms (symmetric and asymmetric key cryptography)

As mention before, all sensors have limited computational power and energy so encryption algorithms and security mechanisms should be lightweight algorithms to decrease computational power, energy and time [11, 36]. But most of encryption algorithms consume power and time. Many researches focus on this problem to decrease computational power and time.

- IoT Privacy (data collection policy and data cleansing)

All information about user behaviour and exchanged data are exposed to several attacks. The challenges of IoT privacy are categorized into data collection policy and data cleansing. Data collection policy depends on the type of collectible data methodology. Data cleansing uses the cryptographic methodology to protect data [40].

- Asymmetric and Complexity

It is hard to manage all devices of the IoT network in the same time because of devices heterogeneity. This leads to that security system becomes weak. Furthermore, the complexity of the IoT environment is resulted from using different devices and applications [36, 40]. These applications need different security mechanisms.

6 IoT Security Layers

IoT security architecture consists of three main layers which can be categorized into perception, network and application layers. Each layer has its own components, communication standards and protocols. The IoT security layers provide different security protocols, services and security mechanisms to enhance the overall protection of the IoT system. So each layer tries to achieve its main goals which are information security, physical security and security management system. The following figure shows the IoT security layer architecture [36]. The following sections display components, functions, common attacks, problems and security measure of each security layer. So we will articulate the problems, different type of attacks and some security solutions of each IoT security layer. Figure 2 presents attacks and countermeasures on each security Layer of IoT.

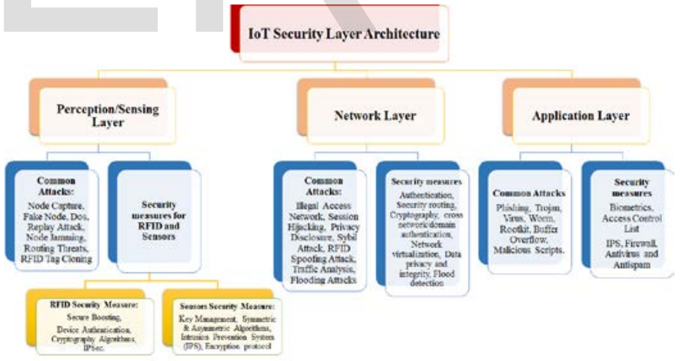

IoT Security Layer Architecture
Perception/Sensing Layer
Network Layer
Application Layer
Common Attacks: Node Capture, Fake Node, Dos, Replay Attack, Node Jamming, Routing Threats, RFID Tag Cloning
Security measures for RFID and Sensors
RFID Security Measure: Secure Booting, Device Authentication, Cryptography Algorithms, IPSec.
Sensors Security Measure: Key Management, Symmetric & Asymmetric Algorithms, Intrusion Prevention System (IPS), Encryption protocol
Common Attacks: Illegal Access Network, Session Hijacking, Privacy Disclosure, Sybil Attack, RFID Spoofing Attack, Traffic Analysis, Flooding Attacks
Security measures Authentication, Security routing, Cryptography, cross network domain authentication, Network virtualization, Data privacy and integrity, Flood detection
Common Attacks Phishing, Trojan, Virus, Worm, Rootkit, Buffer Overflow, Malicious Scripts.
Security measures Biometrics, Access Control List IPS, Firewall, Antivirus and Antispam

Fig. 2. Attacks and Security Measures on each security Layer of IoT

Table 1
Security Layers Specifications and their Security Methods

Layer	Components	Functions	Attacks/ Problems	Security Requirements	Security Methods/ mechanisms
Perception Layer	All types of sensors, RFID, GPS, Bluetooth	It is used to link different smart devices in IoT, collect information, and transmit data to network layer.	Node Capture, Fake Node, Denial of Service (Dos), Replay Attack, Node Jamming, Routing Threats, RFID Tag Cloning, Others	Confidentiality, Integrity, Availability, Authentication, Privacy	Hash Algorithms, Cryptography Algorithms, Access Control, IPSec., Key Management (PKI), Intrusion

					Prevention System (IPS), Encryption Protocol, Risk Assessment
Network Layer	Mobile communication and the Internet	It is used to transmit information transmission	Attacks: Session Hijacking, Sybil, RFID Spoofing, Traffic Analysis And Flooding Attacks. Problems: Compatibility, Cluster Security, Illegal Access Network And Privacy Disclosure	Integrity, Availability, Confidentiality	End to End authentication, Security aware and routing, Cryptography algorithms, Cross-network/domain authentication, Network virtualization technology, Data privacy and integrity to fix and control errors, Flood detection.
Application Layer	Intelligent Community	It is used to provide many services and information analysis	Data access permission, Data protection and recovery, The ability of dealing with mass data and software vulnerabilities	Privacy, Authentication, Authorization, Access control	Biometrics, Access control lists (ACLs), IPS, Antivirus and Anti-spam and Firewall.

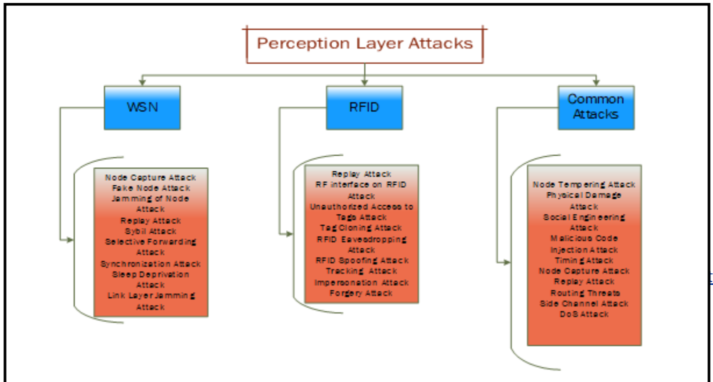
Table 1 shows component and functions of each IoT security layer. It displays attacks, problems and security requirements which are required for each layer. Moreover, table 1 illustrates many security methods to solve security problems in the IoT system. With respect to the security requirements, they provide a high level of security system for the IoT network and enhance the IoT network performance. The following sections will explain attacks and the most common problems categories for each layer. Furthermore, the security measure for each security layer will be explained.

6.1. Perception Layer

As mention above, data are collected from different devices and transmitted through a wireless network. Data are converted to signals which are exposed to many threats. Attackers can easily gain access, monitor, and destroy data and equipment.

6.1.1. *The Perception Layer Attacks Categories*

As mention above, the main components of the perception layer are RFID and WSN so this paper will concentrate on common attacks in WSN, RFID and some effective attacks in the perception layer as shown in figure 3.



The perception layer attacks and threats can be classified into WSN attacks, RFID attacks and the most common attacks in perception layer.

First; the following sections present some WSN Attacks [79, 36, 55, 3, 81].

- Node Capture attack

This type of attack may destroy WSN or sensor node by sending or receiving data to access and change sensitive information. Attacks may control key nodes or gateway nodes. This attack may leak information and threaten the entire network.

- Fake Node Attack

An attacker adds or injects fake node to the IoT system. Then attacker puts fake code or data in the IoT network. This type of attack may stop data transmission, consume the power of nodes and destroy the network.

- Jamming Node Attack

It is the famous attack in the WSN. Attackers try to get involved access in the radio frequencies of nodes. Then it blocks the signals and leads to stop communication of nodes and IoT services.

- Replay Attack

The target of this attack is to break the authentication process to be an authenticated user. The scenario of this attack is that an attacker sends large number of messages which have been received by the destination host. So an attacker may change or replay node by spoofing the information of users.

- Sybil Attack

An attacker intends to control nodes in WSN to make them accept false information to deal with the wrong node in the attacks' network. This type of attack leads to reduce distributed storage and has an influence on multipath routing and topology maintenance.

- Dropping Attack

It is the most dangerous attack in WSN which uses two ways; selective forwarding and synchronization attacks. With regard to the selective forwarding attack, an attacker selects some packets and forwards them to attackers' network and drops the rest of packets to achieve his/her malicious purpose. Thus some nodes can't forward packets. Regarding synchronization attacks, "Synchronization attacks intend to extend its slots of MAC protocols and propagate them to other nodes" [55].

- Sleep Deprivation Attack

In this attack, an attacker consumes batteries lifetime of sensor node by making them busy all the time. This attack influences on the performance of the IoT system and service.

- Link Layer Jamming Attack

The target of this attack is to predict received packets by using MAC protocol in WSN. This attack focuses on the transmission signal of WSN nodes.

Second; the following sections present some RFID Attacks [3, 81, 67, 44, 72, 55, 36, 79].

- RF interface on RFID Attack

This attack depends on DoS attack to use noisy signal and sends it through a radio frequency signal. This leads to stop communication.

- Unauthorized Access to Tag Attack

The target of unauthorized access to tag attack is to break the authentication process to get access to RFID tag. An attacker can read, modify or delete data.

- Tag Cloning Attacks

An attacker can create a duplicate tag so the user can't differentiate between original or fake tag. Subsequently, a user can send or receive fake information and an attacker can capture the original tag to be an authenticated user.

- Replay Attack

The goal of this attack is that an attacker can retrieve data and write data on card of attack using microprocessors. In this case, an attacker gains access to permission of system. Then an attacker becomes authenticated user and access to data or modify data.

- RFID Eavesdropping Attack

An attacker can easily eavesdrop data from tag to user or user to tag to break the confidentiality and get all information. The characteristics of RFID eavesdropping attack is the same as WSN eavesdropping attack because RFID has the same characteristics as WSN.

- RFID Spoofing Attack

The idea of this attack is that attacker can spread wrong data on RFID system and make RFID believe that it is original data. The sender and receiver deal with wrong data so an attacker can get access to data and control the network.

- Tracking Attack

It is dangerous attack because attacker can read RFID tag or private information. The target of tracking attack is to collect information about the IoT network using port scanning tools.

- Impersonation Attack

An attacker can detect a device in the network and impersonate the personality of user. Then attacker generates packets which contain sensitive information or characteristics of device. The purpose of this attack is to change RFID information. This process is known as an interception or fake legitimate identity. The impersonation attack leads to information disclosure.

Third; the most common attacks in perception layer.

- Node Tempering Attack

This type of attack can damage sensor node by sending and receiving data to or from the IoT system to gain access and control all important information.

- Malicious Code Injection Attack

An attacker can perform his/her tasks using MIM attack and put himself or herself between two nodes. An attacker can inject a malicious code into a node to get access to the system and control or damage data.

- Physical Damage Attack

The goal of this attack is to damage and destroy the IoT network. An attacker may manipulate and exploit the IoT network devices to damage the security system of the network and services.

- Social Engineering Attack

An attacker exploits users of IoT network to obtain private information using eavesdropping and sniffing tools.

- Encryption Attack

There are three types of encryption attacks which can be classified into timing attack and side channel attack.

- Timing Attack

It can be implemented by analysing the time of encryption algorithm which is required to implement the encryption mechanism. The goal of this attack is to get key encryption.

- Side Channel Attack

An attacker tries to find the encryption key which is used to encrypt and decrypt data to gain access to data. The serious consequences of this attack are consuming time and energy and leakage of information.

- Routing Threats

It is implemented by resending routing information and creating routing loops. This attack causes the following damages:

1. Controlling and blocking network transmission.
2. Increasing error of messages thus the network path will expand.
3. Increasing end-to-end delay.

- DoS Attack

It is common well known in the IoT network and causes loss of network resources or services and consume bandwidth. DoS attack was discussed in details in the previous section.

6.1.2 Security Measures of the Perception Layer

The previous section discussed many different types of threats and attacks in WSN, RFID and the most common attacks in the perception layer. The security measures are necessary to improve the security level of the IoT system because smart objects of IoT need to be secured with high performance rate. The security measures should provide low power consumption and time. The security measure for perception layer is divided into two items; the security measures for WSN and the security measure for RFID. Table 2 and 3 show comparison among the security measures for WSN and RFID to draw a logical conclusion to select the most suitable security mechanism for WSN RFID with low power and time consumption. Table 2 and 3 present that every security mechanism achieves the security requirements and prevents attacks. In addition to that the following table illustrate advantages and disadvantages of the security measures.

The security measures for WSN

WSN should be protected using security measures to provide the security requirements such as confidentiality, integrity, availability, integrity, privacy and authentication. The security measures provide more convenient security mechanisms to decrease time and power consumption. [26, 36, 11, 55, 45, 81].

TABLE 2
THE SECURITY MEASURES FOR WSN

WSN Security Measures	Usage	Security Requirements	Attack Prevention	Advantages	Disadvantages
Key Management	It is used to provide key generation and update security algorithms using key distribution such as public key infrastructure (PKI) which creates digital certification public keys.	Confidentiality, authentication and availability	Tampering problem, Sybil, eavesdropping and spoofing attacks	It is lightweight security mechanisms	It consumes time
Secure Key Algorithms	Symmetric and asymmetric key algorithms are used for the IoT system. There are many symmetric algorithms such as RC5 and asymmetric algorithms such as AES.	Confidentiality, authentication, integrity and privacy	Replay, traffic analysis, Eavesdropping and spoofing attacks	Symmetric key algorithms provide less power consumption, cost and time of nodes	Asymmetric key algorithms consume more power and time
Security Routing Protocol	There are many of security routing algorithms such as data fusion, multihops routing and key mechanisms. The Secure Network Encryption Protocol (SNEP) is widely used for WSN which achieves point to multi-point broadcast authentication.	Confidentiality, authentication and integrity	Routing threats	SNEP achieves less time	Most of security routing protocol algorithms consume power and time
Authentication and Access Control	Authentication technique is based on lightweight public key authentication technology such as pre shared key and hash function. Access control is based on asymmetric and symmetric cryptosystem. It is necessary to provide high processor speed and memory	*Authentication provides authentication and integrity *Access control provides confidentiality, availability and privacy	Eaves-dropping, node capture and Sybil attacks	Lightweight pubic key authentication technology consumes less power	Traditional authentication and access control mechanisms are not applicable for IoT system
Intrusion Detection and Prevention System IDS/IPS	It provides mentoring the behavior of network and users. It used to detect and prevent most of suspicious user and attacks	IDS and IPS provide most of the security requirements	Most of attacks and threats	IPS is used to detect and prevent attacks and threats. It is used to stop attacks automatically	IDS requires definition of security policy to ensure that threats and attacks are handled according to corporate security policy guidelines

The security measures for RFID

The second important device in the perception layer is RFID. The security measures of RFID are the most significant topic for RFID to provide confidentiality, integrity, availability, integrity, privacy and authentication [79, 49, 67]. Table 3 shows the security measures for RFID, advantages and disadvantages.

TABLE 3

THE SECURITY MEASURES FOR RFID

RFID Security Measures	Usage	Security Requirements	Attack Prevention	Advantages	Disadvantages
Access Control	It is used to secure the sensitive data of users and protect all information of RFID tags. It is used for predicting unauthorized access to tags.	Confidentiality, authentication and integrity	Eavesdropping, spoofing, impersonation and Un-authorized access to Tags attacks	It is useful for chip protection and antenna analysis.	Access control may consume more time
Data Encryption	It is the most significant method to encrypt RFID signal and RFID data.	Confidentiality, integrity and privacy	RF interface on RFID, replay, RFID eavesdropping and spoofing attacks	It uses less computing power and achieve high security level	It consumes more time
IP security (IP-Sec.) mechanism	It offers two levels of security techniques which are authentication and encryption mechanisms. Authentication mechanism: it is used to identify user identity. Encryption mechanism: it is used to encrypt RFID data and signal.	*Authentication process provides integrity, privacy and authentication. *Encryption process provides confidentiality	Eavesdropping, spoofing, data tempering and tag cloning attacks	It gives more secure RFID data and signal.	It consumes power and time
Cryptography technology	It is based on hash function and encryption algorithms. It is used to protect RFID signal	confidentiality, authentication and privacy	RFID Eavesdrop, RFID spoofing, tag cloning, RF interface on RFID and tracking attacks	It protects communication protocols	It consumes more power and time

Table 2 and 3 show the comparison among security mechanisms of WSN and RFID to choose the suitable security measures for data transmission and signals to provide confidentiality, authentication and integrity. These tables are used to select the security algorithms which provide secure data and encrypt RFID signals with low power and time consumption. Each security measure of WSN and RFID provides security requirements to produce high performance rate. In addition to, table 2 and 3 display advantages and disadvantages of security measures to develop security mechanisms. Moreover, table 2 and 3 explain that security measures for WSN and RFID can prevent the most dangerous attacks.

There are other security methods for the perception layer which are shown in the following sections [81, 49, 3].

- Secure Booting

Cryptographic hash algorithms are used to check IoT devices and software by using the digital signature. This security mechanism is inappropriate for IoT system because it needs power and time.

- Anonymity

Anonymity is the best solution for the IoT network to protect the private information of users. The shortcoming of anonymity is that it needs more processing power.

- Risk Assessment

It is an important method to protect the IoT network and prevent many threats and attacks. Risk assessment is the most significant method for the IoT network because it is able to discover any error in the security system. It has the capability for detecting any threats and attacks in IoT devices using many techniques such as IPS. Risk assessment provides many security mechanisms which are appropriate methods for the nature of IoT environment. The security mechanisms should provide low consumption of power and time to achieve high performance rate of the IoT network. Therefore; the security algorithms need to modify, improve and enhance to be convenient algorithms for smart objects of the IoT system.

6.2. Network Layer

As mention above, the main equipment of the network layer are mobile communication network and the Internet. The network layer deals with data, transmission mediums and communication protocols. It is considered fertile land for many threats, attacks and problems.

6.2.1 The Network Layer Attacks and Problems

In the network layer; an attacker tries to gain access to transmitted information, transmission mediums and communication protocols. The purpose of attacker is destroy confidentiality and integrity. The next sections will explain the problems of the network layer. Figure 4 illustrates the classifications of attacks and problems of the network layer.

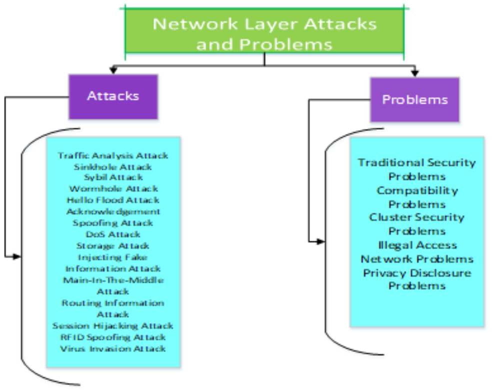


Fig. 4. Network Layer Attacks and Problems Classification

The following sections are divided into two parts which are the network layer attacks and the network layer problems.

1. The network layer attacks

There are many attacks in the network layer which harm the transmitted data, transmission mediums and protocols. The following sections show different types of attacks [3, 49, 44, 55, 6, 67, 72, 11, 36, 79].

- Traffic Analysis Attack

The scenario of this attack is that an attacker tries to capture more information about users and network using some tools such as port scanning and sniffing attacks.

- Sinkhole Attack

An attacker exploits any weak node and controls it. In the same time, this attacker makes this node more trusted and attractive to other neighbor nodes. It can drop all packets and stop data transmission. So sinkhole attack can deny network services and consume power and time. This kind of attack leads to DoS attack which is the most dangerous attack.

- Sybil Attack

This type of attack is very dangerous attack, especially in WSN. An attacker may threaten any node in WSN and represents it with large number of identification. In this time, this node can accept false information and has effect negatively on the IoT network.

- Wormhole Attack

This attack doesn’t depend on the link layer or need to decrypt the encrypted packets. This attack can manipulate the original bit of channel which has a link with low latency. An attacker can relocate the original place of bits in the communication channel with false bits and get access to the IoT system.

- Hello Flood Attack

The hello flood attack is a very risky attack in the IoT network. It has been accomplished using spoofing routing loops. An attacker can send a large number of messages from malicious node to many nodes in the IoT network. This attack causes traffic jamming and blocks the communication channel.

- Acknowledgment Spoofing Attack

Acknowledgment spoofing attack is used for the selective forwarding attack to control any node in the IoT network to achieve attackers’ target. So many packets are lost.

- DoS Attack

An attacker sends a large number of messages or packets to flood network in order to make network resources and services unavailable. It causes also consuming bandwidth, overloading the system and preventing most of the legitimate requests from authenticated and authorized users.

- Storage Attack

All users in the IoT system need to store their private information in many devices or clouds. Therefore, many attacks exploit these devices to gain access and control data.

- Injecting Fake Information Attack

In this attack, an attacker can manipulate one node in WSN and inject malicious information into the IoT network. Therefore, an attacker can access the network and get full control the IoT network.

- Man-In-The-Middle Attack

As mention above, an attacker puts himself/herself between two sensor nodes and eavesdrop all information to get access to information about two sensor nodes. The aim of this attacker is to use the communication channel or protocol to violate privacy and confidentiality.

- Routing Information Attack

The goal of routing information attack is to spoof and change routing information. This attack causes many problems such as sending false messages and errors, dropping network traffic and creating fake routing loop to damage the IoT network.

- Session Hijacking Attack

An attacker attempts to steal session between two nodes to get access and control all information of users and network.

- RFID Spoofing Attack

This attack harms RFID signals. An attacker captures the transmitted data using spoofing RFID signals and makes them authenticated. An attacker uses these signals to transmit malicious data which is considered trusted data.

2. The network layer Problems

The network layer suffers from many problems which cause traffic jamming, network congestion and privacy disclosure [11, 36, 49, 79, 49].

- Conventional Security Problems

The IoT network suffers from common security problems such as eavesdropping, DoS, MIM, session Hijacking, virus invasion and illegal access network which harm confidentiality and integrity.

- Compatibility Problem

As mention above, IoT includes heterogeneous devices so there are multi-paths and multi-access methods. Due to this heterogeneous nature, security system and network coordination are weak. This problem causes that the IoT network is exposed to many different attacks and vulnerabilities.

- Privacy Disclosure

Privacy disclosure is the biggest challenge in the IoT system. An attacker can capture or steal private data of users [Ex. IP address, location, etc] by using social engineering, eavesdropping and sniffing attacks.

- Cluster Security Problem

The cluster security problem is the main problem in the network layer because the IoT network has a large number of devices. Each device generates data. Thus all devices send a huge amount of data. This leads to use a large amount of data traffic which causes network congestion and blocks network traffic.

6.2.2 Network Layer security measures

The security measures of the network layer concentrate on achieving two major security requirements which are data confidentiality and integrity. The security measures of the network layer indicates the appropriate security mechanisms to achieve the security requirements and prevent attacks. The table 4 shows different security measures of the network layer [44, 3, 79, 49, 36].

TABLE 4
THE SECURITY MEASURES FOR THE NETWORK LAYER

Security Measures	**Usage**	**Security Requirements**	**Attack Prevention**	**Advantages**	**Disadvantages**
End to End Authentication and Key Management	All nodes in the IoT network should be authenticated using authentication mechanism, public key infrastructure and End-to-End encryption	Confidentiality and data integrity	Illegal access to node, DoS and Sinkhole attacks	It provides End-to-End authentication and encryption	It is heavy security mechanism.
Security Aware and Routing	The next step of the network layer security measures is security aware and routing which comes after authentication process. The security routing mechanisms are important to secure data and save data privacy.	Confidentiality and data integrity	Most of threats and attacks	It provides multi-paths for data routing and enhance system capability for detecting any error in system	It consumes time
Cryptography System	It used to check data transmission through other nodes and detect any error in network.	Data integrity	It prevents data tempering at received node	It can detect network error and check data. Symmetric key cryptography consumes low power and time	Asymmetric cryptography consumes power and time
Cross-network and domain authentication	Cross-network authentication is used to protect protocols. Cross domain authentication is used to secure DNS	Confidentiality and integrity	Routing threats	It is used to protect network protocols	It consumes more power
Network Virtualization technology	1. It is the process of combing hardware and software resources and network functionality into a single or a virtual network. 2. There are two type of virtual network that are external and internal virtualization. 3. External virtualization combines many network parts into a virtual unit such as LANs to improve network accuracy and data efficiency. 4. Internal virtualization provides network functionality to software on a single network server	Confidentiality and integrity	Most of network attacks	It is used to decrease the complexity of network management	It consumes time
Data privacy and integrity	It is used to detect and control any error which occurs in network. Data integrity uses encryption algorithms to check the original data which is sent to the receiver side	Integrity	Illegal access and spoofing	It is used for checking the original data	It consumes time

Flooding Detection	The idea of this technique is that sender sends hello message to receiver which is used to check the strength of signal. If this signal is similar to the singles in the range of radio the receiver accepts the messages	Confidentiality	Flood attack	It is used to check the original signals	It consumes time

6.3 Application Layer

As mention above, the main equipment of the application layer is an intelligent community. Attackers' goals are data and services such as control of the applications, damage of services, switching off /on servers (e.g. smart grid application) and information theft of a user.

6.3.1 The common problems and attacks of application layer

The following sections presents different attacks and problems of the application layer [3, 45] : -

- Data access permissions

There are a large number of users using different applications. Therefore, there are many holes for software vulnerabilities such as encryption attacks, spam and malicious.

- Data protection and recovery

Data protection and processing mechanisms are not adequate to prevent data loss and damage. So IoT network needs node management system.

- The ability of dealing with mass data and the application software vulnerabilities

There are network interruption and data loss because of a large number of nodes, a huge amount of data transmission and complex environment.

- The application software vulnerabilities

There are many software vulnerabilities such as phishing, Trojan, virus, worm, rootkit, buffer overflow, malicious scripts.

6.3.2 Application Layer security measures

There are two main security measures of the application layer which are biometrics and access control lists (ACLs). Biometrics provides protection of information and prevents internal and external attacks. ACLs can set up roles to allow authenticated and authorized users requests to access network. ACLs can monitor and control the network traffic. The tools of security measures are IPS, Antivirus and Anti-spam and Firewall.

From the above security solutions of the IoT security layers, we can identify the security solution for IoT which are summarized in the following: -

1. IoT network security using Firewall, IPS, etc.
2. Authentication using digital signature and biometrics.
3. Securing Communication using PKI authentication and encryption.
4. Securing Execution of code using cryptography algorithms and software tools.
5. Securing data storage using encryption and authorization
6. Increasing the awareness of safety.

Returning to the previous comparisons posed at this study, it is now possible to present the proposed model of security management for the IoT network.

7 PROPOSED MODEL

The goal of the proposed model is to build security management system for the IoT network to decrease time and power consumption and provide suitable security mechanisms for the IoT security layers. The proposed model helps researchers and designers to select the convenient protocols and security mechanisms for each security layer to secure data and smart objects. The proposed model is used to prevent or decrease attacks, threats and problems as much as possible. The targets of the proposed model can be presented as follows:

1 It presents clarification study for selecting the suitable security mechanisms for the IoT security layers and explains the advantages and disadvantages of the security mechanisms.

2 It provides secured multiple applications.

3 It provides security requirements such as access control, routing control, authentication, privacy and integrity for each security layer.

4 It provides trusted functionalities for every smart object in IoT, IDS/IPS and security recovery.

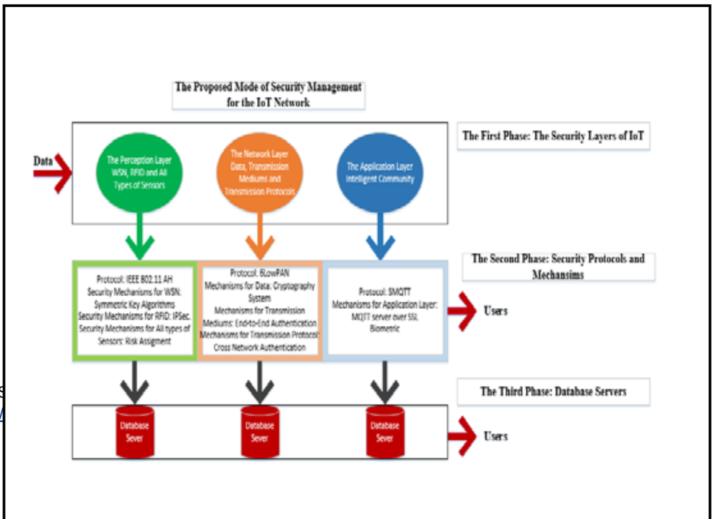
5 It detects and prevents most threats and attacks.

6 It protects the private information of users.

7 It detects any error in data transmission.

In the proposed model, we use Things Board platform which provides many security mechanisms. We can manage the strategy of selection security algorithms to achieve high level of security requirements and decrease power consumption and time.

The stages of the proposed model consist of three phases. The first phase is the security layers of IoT which are perception, network and application layers. The second phase presents the security protocols and mechanisms of the IoT security layer. The third phase contains the database servers which are used for each IoT security layer to store all information about security mechanisms. The database servers are useful for administrator and users to save log files of the security methods and users.


The Proposed Mode of Security Management for the IoT Network
The First Phase: The Security Layers of IoT
Data
The Perception Layer WSN, RFID and All Types of Sensors
The Network Layer Data, Transmission Mediums and Transmission Protocols
The Application Layer Intelligent Community
The Second Phase: Security Protocols and Mechansims
Protocol: IEEE 802.11 AH Security Mechanisms for WSN: Symmetric Key Algorithms Security Mechanisms for RFID: IPSec. Security Mechanisms for All types of Sensors: Risk Assigment
Protocol: 6LowPAN Mechanisms for Data: Cryptography System Mechanisms for Transmission Mediums: End-to-End Authentication Mechanisms for Transmission Protocol: Cross Network Authentication
Protocol: SMQTT Mechanisms for Application Layer: MQTT server over SSL Biometric
Users
The Third Phase: Database Servers
Database Sever
Database Sever
Database Sever
Users

7.1 The First Phase of the proposed Model

The first phase of the proposed model has been discussed in the previous sections so we will concentrate on the second and the third phases.

7.2 The second Phase of the proposed model

The second phase is divided into three main sections. These sections describe the used protocols and security mechanisms of the IoT security layers respectively.

7.2.1 The first section of the second phase describes the used protocol and security mechanisms of the perception layer.

The most suitable protocol for the perception layer is IEEE 802.11 AH because it is the suitable for wireless communication. It is a light protocol and consumes low power and time. In the same time, it decreases the overhead problem. It provides efficient bidirectional exchanged packet to allow sensor to save more power using uplink and downlink communication between sensors. A sensor sends data and goes to sleep when sensor finishes its mission. It has a short MAC frame which is used to increase the sleep time to save power. IEEE 802.11 AH uses the encryption algorithm to provide confidentiality and privacy.

The convenient security mechanisms of the perception layer can be identified according to the previous survey of security mechanisms which were explained in table 2 and 3. Table 2 and 3 displayed the advantages and disadvantages of each security mechanisms to provide the suitable selection security mechanisms for WSN and RFID. The appropriate security mechanisms of WSN are Key Management (PKI) and secure key algorithms using symmetric key algorithms which provide low power consumption. IPSec. Mechanism is used for RFID because it provides authentication and encryption algorithms.

For authentication algorithms, access token is used to provide one-way hash function. One way hash function allows users to enter usernames and passwords in order to obtain access token to get a specific resource without using their username and password. Once user obtain access token, user can display the access token to gain access to a specific resource for a period of time to the remote site. The client must specify the access token as part of request URL or as username. Access token based on authentication algorithm provides authorization, access control, availability and confidentiality.

For encryption algorithm, the symmetric algorithm is used for achieving a lightweight encryption algorithm to produce low power and time. Anonymity and risk assessment are used for all types of sensors to protect the private information of users and detect the network errors.

7.2.2 The second section of the second phase describes the used protocol and security mechanisms of the network layer

The most appropriate protocol of the network layer is 6LowPAN which is used to encapsulate IPV6. IPV6 provides long header in small packet. 6LowPAN provides low bandwidth, low power consumption, low cost, mobility, unreliability, scalable networks and long sleep time. It can reduce transmission overhead problem.

The suitable security mechanisms of the network layer can be classified into the security measure of data transmission, transmission mediums and transmission protocol which was explained in table 4.

Cryptography system is used for securing data transmission using symmetric key cryptography algorithm. It consumes low power and time.

End-to-End authentication algorithm using X.509 Certificate-Based Authentication is used for transmission mediums. It uses two-way Socket Secure Layer (SSL) connection to generate a client-side certificate and connect to server. It uses PKI mechanism because there is no need to distribute public keys or validate fingerprints when creating or updating key pairs. It is highly scalable implementation because it doesn't need to trust individual entities but it needs a single Certificate Authentication (CA) or a limited number of CAs. It provides identity verification through secret private keys.

The cross-network authentication mechanism is used to protect transmission protocol to protect IoT protocols. It is used to decrease the complexity of network management.

7.2.3 The third section of the second phase describes the used protocol and security mechanisms of the application layer

The used protocol is Secure MQTT (SMQTT) protocol using encryption based on lightweight encryption algorithms to achieve low power and time. MQTT server over SSL is the backbone of the IoT network security which protects the sensitive information over the IoT network. SSL protects the IoT applications using encryption algorithms to secure sensitive information, authentication, critical security and data integrity for application interface and personal information about users.

Biometrics is the suitable security measure for the application layer because biometrics can prevent internal and external attacks and protect all data between the application layer and users. Biometrics is new topic in the research area and all researches try to find the suitable security algorithms for IoT network to decrease power consumption and time. In addition to; access control lists are important elements in IoT network to monitor, manage and control network traffic.

7.3 The third phase of the proposed model

The third phase of the proposed model is database servers which store all information and parameters of security mechanisms for each security layer, users' profiles, errors of the security mechanisms, log files of the IoT system and access control lists. The third phase can help an administrator and the users to manage all information about the IoT network and users

The implementation of the proposed model and its variations suitable for different IoT network platforms are the main target of the future work. The impact of the proposed model on the security algorithms and power consumption.

8 Conclusion

The Internet of things (IoT) became the most significant innovation in the world and is a promising innovation to improve our life. In the same time, IoT faces many challenges. The biggest challenge is security and privacy challenges which provide the security requirements. The main goal of the current study was to determine the security requirements which can improve the performance rate of the IoT network. This paper presented briefly the introduction of IoT including the history, components, connections and IoT applications. This study has discussed the IoT security challenges which solve the most of IoT security problems to prevent internal and external attacks. In this study, we reviewed the security requirements to setup rules, laws and terms of service. The security requirements play the most significant role in the design of security solutions and management of the IoT network.

One of the more significant security subjects to emerge from this study is that the understanding of the meaning and ypes of threats, attacks, exposure and vulnerabilities. All these threats are the most part for any security system to detect and prevent them using suitable security methods. The purpose of the current study concentrated on the IoT layers and features to face the IoT security problems. The next major target of this study was description of the IoT security layers. This survey paper described attacks and problems for each IoT security layers and their security measures. This paper presented comparisons among security mechanisms for each IoT security layers which were designed to determine the effect of security measures on the consumption power and time. Therefore, these comparisons had significant influence on the suitable selection of security mechanisms which provide low power consumption and time.

The target of these comparisons presented the proposed model of the security management for the IoT system to select the convenient protocols and security algorithms. The aim of the proposed model is to protect data, transmission mediums, protocols and applications to prevent the most of threats and attacks. The purpose of the proposed model is providing the security requirements and securing multiple applications. The proposed model is used to detect network errors and protect the private information of users. This proposed model can help the designers to manage the security methods in each IoT security layer. The main contribution of the proposed model was to select and manage the appropriate security mechanisms to achieve low consumption power and time.

References

[1] A.Vithya Vijayalakshmi, L. Arockiam, "A Study on Security Issues and Challenges in IoT", International Journal of Engineering Sciences & Management Research (IJESMR), vol. 3, no. 11, pp. 34-43, 2016.

[2] Aanchal Punia, Daya Gupt, Shruti Jaiswal, "A Perspective on Available Security Techniques in IoT", Proc. 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT), India, pp. 1553- 1559, 19-20 May 2017.

[3] Abdul Wahab Ahmed, Mian Muhammad Ahmed, Omair Ahmad Khan, Munam Ali Shah, "A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT", International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 7, pp. 489-501, 2017.

[4] Abomhara, Mohamed, Geir M. Køien, "Security and Privacy in the Internet of Things: Current status and open issue", Proc. The 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, pp. 1-8, 11-14 May 2014.

[5] Ahmad W. Atamli, Andrew Martin, "Threat-based Security Analysis for the Internet of Things", Proc. the 2014 International Workshop on Secure Internet of Things, wroclaw, Poland, pp. 35-43, 10-10 September 2014.

[6] Alma Oracevic, Selma Dilek, Suat Ozdemir, "Security in internet of things: A survey", Proc. the 2017 International Symposium on Networks, Computers and Communications (ISNCC), Marrakech, Morocco, pp. 1-6, 16-18 May 2017.

[7] Andreas Jacobsson, Paul Davidsson, "Towards A Model of Privacy and Security for Smart Homes", Proc. the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, pp. 727 – 732, 14-16 December 2015.

[8] Andy Crabtree, Tom Lodge, James Colley, Chris Greenhalgh, Kevin Glover, Hamed Haddadi, Yousef Amar, Richard Mortier, Qi Li, John Moore, Liang Wang, Poonam Yadav, Jianxin Zhao, Anthony Brown, Lachlan Urquhart, Derek McAuley, "Building Accountability into the Internet of Things: the IoT Databox Model", Springer, Journal of Reliable Intelligent Environments, vol. 4, 39–55, 2018.

[9] Ankush B. Pawar, Shashikant Ghumbre, "A survey on IoT Applications, Security Challenges and Counter Measures", Proc. of the 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, India, pp. 294 – 299, 19-21 December 2016.

[10] Anurag Shukla, Sarsij Tripathi, "Security in Internet of Things", International Journal of Control Theory and Applications (IJCTA), vol. 9, no. 41, pp. 743-752, 2016.

[11] Bhoopathy V., R.M.S. Parvathi, "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks", International Journal of Engineering Research and Applications (IJERA), vol. 2, pp. 466-474, 2012.

[12] Carsten Maple, "Security and Privacy in the Internet of Things", Journal of Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017.

[13] Carsten Maple, M.c. schraefel, Richard gomer, Alper Alan, Enrico gerding, "The internet of things: interaction challenges to meaningful consent at scale", Interactions, vol. 24, no. 6, pp. 26-33, 2017. doi:10.1145/3149025

[14] Chen Long, "Security Management for the Internet of Things", A Thesis of Applied Science at the University of Windsor University of Windsor Scholarship at UWindsor Electronic Teses and Dissertations, 2017, available at https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=6934&context=etd

[15] Chi Lin, GuoweiWu, TieQiu, Jing Deng, "A Low-Cost Node Capture Attack Algorithm for Wireless Sensor Networks", International Journal of Communication Systems, vol. 29, pp. 1251-1268, 2016, available at https://doi.org/10.1002/dac.3097

[16] Cisco, Cloud and Mobile Network Traffic Forecast - Visual Networking Index (VNI), 2015, available at http://cisco.com/c/en/us/solutions/serviceprovider/visual-networking-index-vni/index.html

[17] Dan Dragomir, Laura Gheorghe, Sergiu Costea, Alexandru Radovici, "A Survey on Secure Communication Protocols for IoT Systems", Proc. the 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, Greece, pp. 47 – 62, 30 September 2016.

[18] Danova Tony, "Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020", In: Business Insider, 2 October 2013, available at http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10

[19] Davar Pishva, "Internet of Things: Security and Privacy Issues and Possible Solution", Proc. the 19th International Conference on Ad-

vanced Communication Technology (ICACT), Bongpyeong, South Korea, pp. 797 – 808, 19-22 February 2017.

[20] Dave Evans, “The Internet of Things How the Next Evolution of the Internet is Changing Everything”, white Paper of Cisco Internet Business Solutions Group (IBSG), pp. 1-11, 2014. available at https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[21] D. Bastos, M. Shackleton, F. El-Moussa, 2018.

[22] Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments. Proc.Living in the Internet of Things: Cybersecurity of the IoT, London, UK, pp. 1-7, 28-29 March 2018.

[23] Folasade Osisanwo, Shade Kuyoro, Oludele Awodele, “Internet Refrigerator–A Typical Internet of Things (IoT)”, Proc. the 3rd International Conference on Advances in Engineering Sciences & Applied Mathematics (ICAESAM’2015), London (UK), pp. 59-63, 23-24 March 2015.

[24] Gang Gan, Zeyong Lu, Jun Jiang, “Internet of Things Security Analysis”, Proc. the 2011 International Conference on Internet Technology and Applications, Wuhan, China, pp. 1-4, 16-18 August. 2011.

[25] Hokeun Kim, Edward A. Lee, “Authorization for the Internet of Things”, IT Professional, vol. 19, no. 5, pp. 27-33, 2017.

[26] Hui Suoa, Jiafu Wan, Caifeng Zoua, Jianqi Liu, “ Security in the Internet of Things: A Review”, Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, pp. 648- 651, 23-25 March 2012.

[27] Huawei, “Tap Into New Growth with Intelligent Connectivity”, White paper global connectivity index, 2018, at available at https://www.huawei.com/minisite/gci/assets/files/gci_2018_whitepaper_en.pdf?v=20180716

[28] I.Lakshmi, “The Internet of Things (IoT) and Furthermore Cyber Security: Vulnerabilities, Threats, Intruders and Attacks”, IOSR Journal of Computer Engineering (IOSR-JCE), vol. 19, pp. 85-94, 2017.

[29] Jaime Jimenez, Michael Koster, Hannes Tschofenig, “IoT Semantic Interoperability”, Proc. of the Workshop 2016’, San Jose, Us, 17-18 March 2016, available at http://www.ipso-alliance.org/wp-content/uploads/2016/01/ipso-paper.pdf

[30] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, Klaus Wehrle, “Privacy in the Internet of Things: Threats and Challenges”, Security and Communication Networks, vol. 7, no. 12, pp. 2728-2742, 2014.

[31] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, “Internet of Things (IoT): A vision, Architectural Elements, and Future Directions”, Elsevier, Future Generation Computer Systems, vol. 29, pp. 1645–1660, 2013.

[32] Jing Deng, Richard Han, Shivakant Mishra, “Countermeasures against Traffic Analysis Attacks in Wireless Sensor Networks”, Proc. the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, Greece, 5-9 September 2005.

[33] Jing Liu, Yang Xiao, C. L. Philip Chen, “Authentication and Access Control in the Internet of Things”, Proc. the 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Macau, China, pp. 588-592, 18-21 June 2012.

[34] Jon R. Ward, Mohamed Younis, “A Cross-Layer Traffic Analysis Countermeasure against Adaptive Attackers of Wireless Sensor Networks”, Proc. the MILCOM 2016 - 2016 IEEE Military Communications Conference, Baltimore, MD, USA, pp. 271 – 276, 1-3 November 2016.

[35] Jorge Granjal, Edmundo Monteiro, Jorge Sá Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues”, Proc. the IEEE Communications Surveys & Tutorials, vol. 17, pp 1294 – 1312, 2015.

[36] Kai Zhao, Lina Ge, “A Survey on the Internet of Things Security”, Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS), Leshan, China, pp. 663-667, 14-15 December 2013.

[37] Keijo Mononen, Patrik Teppo, Timo Suihko, “END-TO-END IoT Security”, Charting the Future of Innovation, Ericsson Technology, 2017, available at https://www.ericsson.com/assets/local/publications/ericsson-technology-review/docs/2017/managing-iot-security-end-to-end-etr-10-2017.pdf

[38] Keyur K Patel, Sunil M Patel, “Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges”, International Journal of Engineering Science and Computing, vol. 6, no. 5, pp. 6122- 6131, 2016..

[39] Khaled M. Elleithy, Drazen Blagovic, Wang Cheng, Paul Sideleau, “Denial of Service Attack Techniques: Analysis, Implementation and Comparison”, Systemics, Cybernetics and Informatics, vol. 3, no. 1, pp. 66-71, 2006.

[40] Krishna Kanth Gupta, Sapna Shukla, “Internet of Things: Security Challenges for Next Generation Networks”, Proc. the 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016), Noida, India, pp. 315-318, 3-5 February 2016.

[41] Ludwig Seitz, Goran Selander, Christian Gehrmann, “Authorization Framework for the Internet-of-Things”, Proc. the 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Madrid, Spain, pp. 1 – 6, 4-7 June 2013.

[42] Luigi Atzori, Antonio Iera, Giacomo Morabito, “The Internet of Things: A Survey”, Elsevier, Computer Networks, vol. 54, pp. 2787–2805, 2010..

[43] M. Vivekananda Bharathi, Rama Chaithanya Tanguturi, C. Jayakumar, K. Selvamani, “Node Capture Attack in Wireless Sensor Network: A Survey”, Proc. the 2012 IEEE International Conference on Computational Intelligence and Computing Research. Coimbatore, India, pp. 1 – 3, 18-20 December 2012.

[44] M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IoT)”, International Journal of Computer Applications, vol. 111, no. 7, pp. 1-6, 2015.

[45] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, “A Review on Internet of Things (IoT)”, International Journal of Computer Applications, vol. 113, no. 1, pp1-7, 2015.

[46] Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, Mischa Dohler, Standardized Protocol Stack for the Internet of (Important) Things. IEEE Communications Surveys & Tutorials, vol. 15, pp. 1389 – 1406, 2013.

[47] Mario Collotta, Giovanni Pau, “A Solution Based on Bluetooth Low Energy for Smart Home Energy Management”, Journal of Energy Research, Engineering and Policy, vol. 8, no. 10, pp.11916-11938, 2015.

[48] Maryam Daud, Quratulain Khan, Yasir Saleem, “A Study of Key Technologies for IoT and associated Security Challenges”, Proc. the International Symposium on Wireless Systems and Networks (ISWSN), Lahore, Pakistan, pp. 1-6, 19-22 November 2017.

[49] Mian Muhammad Ahemd, Abdul Wahid, “IoT Security: A Layered Approach for Attacks & Defenses”, Proc. the International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, pp. 104-110, 19-21 April 2017, doi: 10.1109/COMTECH.2017.8065757

[50] Mikko Lehtonen, Daniel Ostojic, Alexander Ilic, Florian Michahelles, “Securing RFID Systems by Detecting Tag Cloning”, Proc. the International Conference on Pervasive Computing, Berlin, Germany, pp. 291-308, 2009.

[51] Mohamed Abomhara and Geir M. Køien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks”, Journal of Cyber Security, vol. 4, pp. 65-88, 2015.

[52] Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu, “Authentication Protocols for Internet of Things: A Comprehensive Survey”, Wiley Hindawi Security and Communication Networks, vol. 2017, pp.1-41, 2017.

[53] Muhammad A. Iqbal, Oladiran G.Olaleye, Magdy A. Bayoumi, “A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches”, Global Journal of Computer Science and Technology: E Network, Web & Security, vol. 16, no. 7, pp. 1-11, 2016.

[54] Nikos Fotiou, Theodore Kotsonis, Giannis F. Marias, George C. Polyzos, “Access Control for the Internet of Things”, Proc. the IEEE Conferences, 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, Greece, pp. 29-38, 26-30 September 2016.

[55] Otmane El Mouaatamid, Mohammed Lahmer, Mostafa Belkasmi, “Internet of Things Security: Layered Classification of Attacks and Possible Countermeasures, Electronic Journal of Information Technology, Issue 9, pp. 24-37, 2016.

[56] Pallavi Sethi, Smruti R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications”, Journal of Electrical and Computer Engineering, vol. 2017, pp. 1-25, 2017.

[57] Pavan Pongle, Gurunath Chavan, “A survey: Attacks on RPL and 6LoWPAN in IoT”, Proc. the 2015 International Conference on Pervasive Computing (ICPC), Pune, India, pp. 1 – 6, 2015.

[58] Qi Zhang, AnWang, Yongchuan Niu, Ning Shang, Rixin Xu, Guoshuang Zhang, Liehuang Zhu, “Side-Channel Attacks and Countermeasures for Identity-Based Cryptographic Algorithm SM9”, Hindawi Security and Communication Networks, vol. 2018, pp.1-14, 2018.

[59] Rinju Ravindran, Jerrin Yomas, Jubin Sebastian E, “IoT: A Review on Security Issues and Measures”, Engineering Science and Technology: An International Journal (ESTIJ), vol. 5, no. 6, pp. 348-351, 2015.

[60] Rob van Kranenburg, Alex Bassi, “IoT Challenges. mUX”, Journal of Mobile User Experience, Communications in Mobile Computing, vo. 1, pp.1-9, 2012.

[61] Rolf H. Weber, “Accountability in the Internet of Things”, Computer law & security review, vol. 27, no. 4, pp. 133-138, 2011.

[62] S. Daneshmand, A. Jafarnia-jahromi, A. Broumandan, G. Lachapelle, “A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array”, Proc. the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012). Nashville Convention Center, Nashville, Tennessee, USA, pp. 1233 – 1243, 17 – 21 September 2012.

[63] Sarvesh Kumara, Suraj Pal Singhb, Ashwanee Kumar Singhc, Jahangir Ali, “Virtualization, the Great Thing and Issues in Cloud Computing”, International Journal of Current Engineering and Technology, vol. 3, no. 2, pp. 338–341, 2013.

[64] Somayyeh Jafarpour, Ammar Yousefi, “Security Risks in Cloud Computing: A Review”, International Journal of Current Engineering and Technology, vol. 6, no. 4, pp. 1174-1179, 2016.

[65] S.Harini, K.Jothika, K.Jayashree, “A Survey on Privacy and Security in Internet of Things”, International Journal of Innovations in Engineering and Technology (IJIET), vol. 8, pp. 129-134, 2017.

[66] Salavat Marian, Popa Mircea, “Sybil Attack Type Detection in Wireless Sensor Networks based on Received Signal Strength Indicator detection scheme”, Proc. the IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics. Timisoara, Romania, pp. 121-124, 21-23 May 2015.

[67] Sathish Alampalayam Kumar, Tyler Vealey, Harshit Srivastava, “Security in Internet of Things: Challenges, Solutions and Future Directions”, Proc. the System Sciences (HICSS), 49th Hawaii International Conference on System Sciences, Koloa, HI, USA, pp. 5771- 5780, 5-8 Jan. 2016.

[68] Shahid Raza, Tómas Helgason, Panos Papadimitratos, Thiemo Voigt, “SecureSense: End-to-End Secure Communication Architecture for the Cloud-Connected Internet of Things”, Future Generation Computer Systems, vol. 77, pp. 40-51, 2017.

[69] Sharon L. Poczter, Luka M. Jankovic, “The Google Car: Driving Toward A Better Future?”, Journal of Business Case Studies, vol. 10, no. 1, pp. 7-14, 2014..

[70] Sneha S. Rana, T. M. Bansod, “IP Spoofing Attack Detection using Route Based Information”, International Journal of Advanced Research in Computer Engineering & Technology, vol. 1, pp. 285-288, 2012.

[71] Soumyalatha, Shruti G Hegde, “Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges”, International Journal of Advanced Networking & Applications (IJANA)”, Proc. the 1st International Conference on “Innovations in Computing & Networking” (ICICN-2016), Raja Rajeswari College of Engineering, Bangalore, India, pp. 477- 482, 12-13 May 2016.

[72] Stuart Millar, “Network Security Issues in the Internet of Things (IoT)”, Queen's University Belfast Research Portal, pp. 1-6, 2016, available at https://pure.qub.ac.uk/portal/files/123692254/StuartMillar_13616005_Network_Security_Issues_In_The_Internet_Of_Things_v3.pdf

[73] Sunakshi Jaitly, Harshit Malhotra, Bharat Bhushan, “Security Vulnerabilities and Countermeasures against Jamming Attacks in Wireless Sensor Networks: A survey”, Proc. the 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, India, pp. 559–564, 1-2 July 2017.

[74] Tara Salman, Raj Jain, Networking Protocols and Standards for Internet of Things in “Internet of Things and Data Analytics Handbook” Hwaiyu Geng, Editor, John Wiley & Sons, Inc., USA, pp. 215-238, 2016, available at https://doi.org/10.1002/9781119173601.ch13

[75] Tejal Hartalkar, Suyog Bhore, Ketki Borawake, Shraddha Naik, “GSM based Home Automation using MQTT”, International Journal of Engineering Technology, Management and Applied Sciences, vol. 3, pp. 93-98, 2015.

[76] Tri-Hai Nguyen, Myungsik Yoo, “A Hybrid Prevention Method for Eavesdropping Attack by Link Spoofing in Software-Defined Internet of Things Controllers”, International Journal of Distributed Sensor Networks, vol. 13, no. 11, pp. 1-9, 2015.

[77] W.Sharon Inbarani, C.Kumar Charlie Paul, W.Andrew Jerome Jeevakumar, “A Survey on Security Threats and Vulnerabilities in Cloud Computing”, International Journal of Scientific & Engineering Research, vol. 4, pp. 1-4, 2013.

[78] Yasirli Amri, Mukhammad Andri Setiawan, “Improving Smart Home Concept with the Internet of Things Concept Using RaspberryPi and NodeMCU”, Proc. the IOP Conference Series: Materials Science and Engineering, vol. 325, no. 2018, pp. 1-10, 2018.

[79] Yassine Chahid, Mohamed Benabdellah, Abdelmalek Azizi, “Internet of Things Security”, Proc. the 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Morocco, 19-20 April 2017. doi: 10.1109/WITS.2017.7934655

[80] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, Hongbin Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things”, IEEE Internet of Things Journal, vol. 4, pp. 1250-1258, 2017.

[81] Zhang Li, Tong Xin, “Threat Modeling and Countermeasures Study for the Internet of Things”, Journal of Convergence Information Technology (JCIT), vol. 8, no. 5, pp. 1163-1171, 2013.

[82] Zhen Ling, Kaizheng Liu, Yiling Xu, YierJin, XinwenFu, “An End-to-End View of IoT Security and Privacy”, Proc. the GLOBECOM 2017-2017 IEEE Global Communications Conference. Singapore, Malay, pp. 1-7, 4-8 December 2017.

[83] Zheng Yan, Peng Zhang, Athanasios V. Vasilakos, “A Survey on Trust Management for Internet of Things”, Journal of Network and Computer Applications, vol. 42, pp. 120–134, 2014.

[84] Zubair A. Baig, “Securing the Internet of Things Infrastructure–Standards and Techniques”, Proc. the 12th Australian Information Security Management Conference, Conferences, Symposia and Campus Events, Edith Cowan University, Joondalup Campus, Perth, Western Australia, pp. 75-81, 1-3 December 2014.