IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 12 (December. 2018), ||V (II) || PP 81-93

Security Issues in IOT

Dr.P.Neelakantan
Dept of Csevnr Vjiet Hyderabad, India
Corresponding Author Dr.P.Neelakantan

Abstract: The expansion of Internet - connected automation offers a number of previously unimaginable opportunities and applications. The Internet of Things (IoT) is a prominent example. IoT is a network system composed of a number of wired or wireless intelligent sensors and applications. The development of IoT took decades. Cyber - attacks, however, have threatened the IoT since its birth; different threats and attacks can cause serious disasters to the network system without the essential security. This makes the security and management of the IoT security system very important. The proposed architecture can be used to provide security management for an IoT network in detail. Finally, summarize the results of the implementation of the proposed architecture of security functions to achieve efficient and strong IoT security.

Keywords: Internet of things (IoT), security, architecture, threats

---

Date of Submission: 29-11-2018 Date of acceptance: 13-12-2018

I. INTRODUCTION

IoT is a wired and wireless network system comprising many software and hardware entities such as manufacturing management, energy management, irrigation for agriculture, electronic commerce, logistics management, medical and health care systems, aerospace surveys, building and home automation, infrastructure management, large - scale deployments and transport. 1].The purpose of IoT is to transform traditional products into related products by taking advantage of data exchange and communication to monitor and control the objectives. Figure 1 shows the IoT concept..

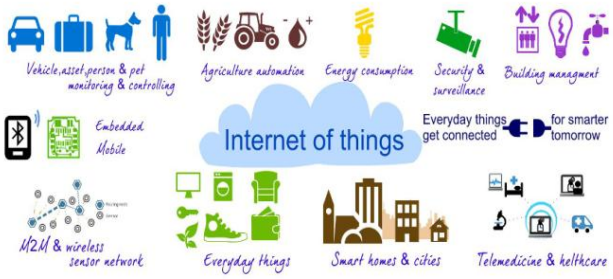

Figure 1. Conception of IoT.

The advantage of the IoT is clear: the collection and exchange of data is efficient. IoT also offers cost - effective means to save energy and contribute to the protection of the environment. In other words, IoT enables advanced security by connecting physical and virtual devices based on existing and evolving interoperable ICT*. 1.2 IoT history As early as 1982, a modified coke machine was manufactured at Carnegie Mellon University that could report both the temperature and the inventory. It is generally thought that this is the first Internet - connected device. Peter T coined the term IoT. Lewis made a speech at the United States Federal Communications Commission (FCC) in 1985. In 1991, Mark Weiser, a chief scientist in the United States and father of omnipresent computing, wrote a seminal paper on omnipresent computing and produced the concept of IoT at academic venues. In 1994, Reza Raji, an Echelon engineer in Palo Alto, California, defined the IoT as " moving small data packets to a wide range of nodes, integrating and automating everything from home appliances to entire factories. " 1] Companies such as Microsoft, Novell and NEST provide some IoT network solutions from 1994 to 1996. In 1999. In 1999. Kevin Ashton, a pioneer in British technology, co - founded MIT's Auto ID Centre. The radio frequency identification (RFID) made the IoT po in its option., security, mobility and convenience are three elements that Internet vehicles should be concerned with.

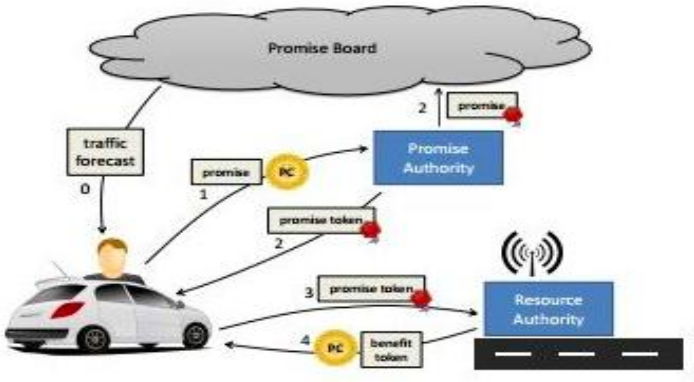

Figure 2: Internet of Vehicles

Safety and security should be the priority objectives for all the features. It involves network security, vehicle-to-vehicle communication security, and vehicle-to-infrastructure communication. The smart sensors guarantee the eco-friendly driving. Another objective is the automatic monitoring and identifying the critical systems and dangers in the road warning. Figure 2 shows a better trip with Internet of vehicles.

1.3.2 Smart Home

Many families now have WIFI devices at home, from their iPhone to their smart TV. The home IP network plays an important role in the smart home, the design of the smart home focuses on comfort, convenience, living arrangements and environmental monitoring. Environmental data such as temperature, lighting, moisture, noise and atmospheric pressure are collected by sensors. The intelligent home application uses these data to control at home air conditioning, lighting, heating, ventilation and safety. Users can modify the smart home application details by using a mobile phone, tablet, laptop or even a voice control system. Figure 3 shows the design of the smart home.

Figure 3: Smart house design

1.3.3 Smart Health

IoT devices may allow remote monitoring of health. Today, not only conventional intelligent health devices are popular on the market, but wearable technology devices such as smart clocks, healthcare devices, fitness tracking devices, wearable babies and pregnancies and even wearable pets are also available. These intelligent healthcare devices are capable of obtaining sensor data. Some other devices support or display the user interface and the wireless network connectivity like Bluetooth or mobile network. Wearable technology equipment requires features such as low power consumption, robustness, durability, accuracy, reliability and privacy. Figure 4 illustrates the understanding of smart health.

Figure 4: Use of IoT in smart health

1.4 Problem of The IoT Security

The security problems descend the pace of IoT development. The attackers can attack the IoT network using different techniques on different layers. When IoT develops, cyber-attacks become more physical threats. Security of data has become a priority for the design of all IoT network systems. Some manufacturers have no safety standards for their products; some devices use their own de facto safety standards that are not compatible with other manufacturing products; some old device versions have no safety measures at all. In automobiles such as breakers, engines, locks and dashboards, computer - controlled devices have been shown to be vulnerable to attackers who have access to the network. Since the IoT is a rich data source, it is always vulnerable to advanced attacks. In 2016, a distributed denial of service (DDoS) attack used IoT devices and caused Mirai to domain a DNS provider and major websites. IoT network system security management is very important for potential end users and network providers.

1.5 Purpose of The Study

The main objective of this study is to provide an IoT security background and then propose a robust IoT security management structure. Research on IoT security management requirements has been published[2][3]. However, a unified approach to addressing the challenges posed by the integration and convergence of IoT into the existing network environment is lacking. To create a more economical and efficient computer - controlled environment. A robust IoT security management system (IoTSMS) is required to integrate new applications that typically require the installation of relevant devices, sensors and software in a seamless manner. The IoTSMS must be able to handle a large number of devices, interconnected systems, transmit and process the security data concerned. IoTSMS is not proposed to develop integrated solutions and incorporate new applications to provide efficient, strong and sustainable IoT security. In this study, we proposed a layered safety functional structure for a strong IoTSMS.

1.6 Importance of the Study

Millions of intelligent devices create enormous amounts of data each day. These data can be used to improve user experience, improve product services and benefit the development of other data - based searches such as fitness and health, automatic driving and business management. 4] We changed our lives on the Internet. The IoT has already assimilated into our daily lives, but much of the public debate about accepting or rejecting the IoT concerns security. The important thing of this study is to provide the IoT with a functional security architecture and easy security management methods to meet the needs of end users and network providers. IoT security management could protect the data from the bottom to the top levels of the IoT; useful data and data protection information are firmly protected by the various security policies, services and mechanisms.

1.7 Scope and Limitations of the Study

This IoT security and management study is a qualitative study. Every design has its own limits. Each layer in the IoT has its own security challenges and problems. Different threats can affect each layer differently. In order to counteract the corresponding security threats, different security services and various security mechanisms had to be implemented in different levels. However, various suppliers and network suppliers and manufacturers can use different safety standards and mechanisms for their own IoT products. Therefore, make the IoT SMS inefficient and unworkable.

1.8 Complexity and Compatibility

The IoT system has 4 layers of architecture. Under various circumstances, such as multi-users and multi-tasks, the workload of the IoT SMS can be difficult. A small bug in hardware or software can cause serious or worse system failure. Therefore, a common standard for IoT in both hardware and software should be used in the design on each layer. IoT compatibility issues should be dealt with by hardware and software manufacturers.

II. SECURITY REQUIREMENTS

2.1. security requirements

The fundamental security problems of IoT require the identity authentication mechanisms and data privacy protection. Data confidentiality, data integrity and data availability are three fundamental areas. Infringement of any of these three basic security areas can damage the IoT system. Each of the four layers of the IoT network system should therefore comply with these minimum standards. Figure 5 shows the basic. requirements of security for IoT

Figure 5: Basic requirements for IoT

2.1.1 Data Confidentiality

The purpose of data privacy is to protect the privacy of sensitive information through the use of certain mechanisms and to prevent unauthorized access[10]. Confidentiality of data means that data collected by sensors and nodes should not be transmitted to an unauthorized party for IoT devices such as sensors and nodes. Data encryption is a confidentiality mechanism for data. The encrypted data converts to cipher text; therefore, unauthorized users cannot access the data easily. Two - stage verification is another way of ensuring confidentiality of data. Users can only access data through two dependent authentication tests in this method.

2.1.2 Data Integrity

Data integrity protects useful information during communication against the tempering of cybercriminals. There are a number of cases, such as server crash or power disruption, which can affect the integrity of data. One method for ensuring data integrity at the first level is the Cyclic Redundancy Check (CRC): CRC is a simple error detector mechanism for encoding the message by adding a fixed-length check value for error detection in IoT communication networks[11] Other methods such as Version Control can synchronize and backup data to maintain system file changes, thereby ensuring data integrity by restoring changing data in the event of deletion or loss.

2.1.3 Data Availability

Data availability is very important for IoT security, data availability ensures that users can access information resources in both normal and disastrous situations and data availability ensures that the information flows accordingly. In order to guarantee data availability and reliability, the IoT system requires backup and redundant techniques to duplicate important information and prevent loss of data in system failure or system conflict. Service Denial (DoS) and Distributed Denial (DDoS) attacks cause data availability security issues, router filtering can counteract the problem.

2.2 Security Mechanisms

The IoT security mechanisms are based on restricted devices such as low - power wireless sensors and network devices with battery power. Therefore, efficient safety mechanisms for IoT security must be taken into account in all designs. Since nodes and sensors are low power consumption and low computing capacity devices, the IoT device safety mechanisms should be as light as possible. The data collected by the nodes can be

captured by intruders or used to destroy the network system without the efficient security. In order to protect the system, several basic safety mechanisms at all levels should therefore be involved.

2.3 Threats and Attacks on Element Layer

Element layer consists of different nodes and sensors to collect the data from connected network environment. The nodes and sensors are exposed to different threats such as unauthorized access, eavesdropping, spoofing, etc.

2.3.1 Unauthorized Access

The Element layer used nodes and sensors like RFID, tags, barcode labels, actuators and intelligent detection devices to collect the data from the environment; due to the absence of authentication services, unauthorized parties can get access to the data and modify it, or even delete the data. [12].

2.3.2 Eavesdropping

The information collected by wireless components such as RFID and tags, as mentioned in the reference, is easy to read by attackers. [3] Attackers may use data to hack any IoT system or to sniff important information, such as password or user confidentiality.

2.3.3 Spoofing

Spoofing is the attackers send some fake information to the nodes and sensors pretend to act like the original failure, then the attackers may have the full access to the system.[6]

2.4 Element Layer Security

Element layer is the lowest layer of the four layers of an IoT system environment. Element layer consists of sensors and nodes, these devices are exposed to threats such as unauthorized access, eavesdropping and spoofing.

2.4.1 Element Layer Security Services

Authentication services protect the element layer against unauthorized attacks by access. Access control services can protect the layer of the element from the attacks. To protect the element layer from spoofing attacks, confidentiality services are required. Authentication, access control and confidentiality services therefore protect the element layer against attacks such as unauthorized access, removal and spoofing.

2.4.2 Element Layer Security Mechanisms

The element layer authentication services are using hash algorithms to provide a digital signature to counter the unauthorized access attacks, the access control table mechanism counter the eavesdropping attacks and the public key infrastructure (PKI) provide the confidentiality of the data collected by the sensors and smart devices.

2.5 Threats and Attacks on Network Layer

The network layer transmits the data collected by the nodes and sensors to the terminal, the wireless sensor network has been used to transmit the data, the network layer has several security concerns, such as denial of services (DoS) attacks, man-in - the-middle attacks and malicious code injection.

2.5.1 Denial-of-Service (DoS)

The DoS attack is when the attackers send a lot of useless data to overflow the network.[5] The IoT system will be blocked for the access of authorized users by the enormous consumption of system resources.

2.5.2 Man-in-the-Middle Attack

This attack is a sort of disappointment that unauthorized attackers can control communication between the parties[7]. Useful information can be obtained via the communication channels.

2.5.3 Malicious Code Injection

In this case, the attacker compromises sensors and vulnerable nodes by injecting malicious codes and attacks the IoT system.[8] The result may cause the network to shut down and the system could be controlled by the attackers.

2.6 Network Layer Security

Network layer transmits the data which collected by the nodes and sensors to the upper layer, which is the service layer. There are several security concerns to be addressed at the network layer, such as denial of services attacks (DoS), man-in-the-middle attacks and malicious code injection.

2.6.1 Network Layer Security Services

The availability and non - denial of service protects the network layer from denial of service attacks, protects the network layer from man-in - the-middle attacks, protects the network layer against malicious code injection attacks.

2.6.2 Network Layer Security Mechanisms

The router filtering uses the availability and non - denial of services to counteract network layer denial of service attacks. The encryption of data was necessary to counter man-in - the-middle attacks and the anti - virus security mechanism needed to counter malicious code injection.

2.7 Threats and Attacks on Service Layer

The service layer processes data and connects the data collected from the element layer to the storage. The security of the service layer should prevent attacks such as DoS, unauthorized access and malicious insiders.

2.7.1 DoS Attack

The DoS attack in the service layer is similar to the network layer, the attackers send lots of useless data to make the network traffic flooded, resulting in an enormous consumption of system resources that exhausts the IoT system and prevents users from accessing it.

2.7.2 Unauthorized Access

Unauthorized attackers could access the service layer providing the data and storage interface to the IoT system, thereby modifying or deleting important data and causing fatal IoT problems.

2.7.3 Malicious insider

The malicious insider attack occurs within the IoT environment that uses personal data. These data are very easy to access from within and can only be accessed by authorized users. 18] This is a different threat from unauthorized access and requires a variety of anti-threat mechanisms.

2.8 Service Layer Security

The service layer processes data and links data collected from the element layer to the storage. The layer of services addresses security issues such as DoS attacks, unauthorized access and malicious insiders.

2.8.1 Service Layer Security Services

Protecting the service layer from denial of service attacks and non - denial of service. Access control and authorizationservice protects the service layer against unauthorized access attacks and the audit log service we can protect the service layer against malicious insider attacks.

2.8.2 Service layer security mechanisms

The availability and non - denial of service via intrusion detection system[19] (IDS) can counteract denial of service attacks. The access control mechanism is used to counter unauthorized access attacks and event monitoring is necessary to counter malicious insider attacks.

2.9 Application Layer threats and attacks

The application layer comprises a variety of IoT applications. The application layer security issues such as DDoS attack, malicious code injection attack and phishing attack need to be addressed.

2.9.1 DDoS Attack

The Denial of Services (DDoS) attack in the application layer is now sophisticated. An attacker can easily break the system for unencrypted devices and cause users data privacy problems. The victims have no access to the system services and have hardly noticed that DDoS attacks have taken place in the IoT system[9].DDoS assaults differ from DoS attacks. Distributed service denial (DDoS) attacks are launched from the various connected devices, which are distributed across the IoT environment.

2.9.2 Malicious Code Injection

Malicious code injection is when attackers hacking the system and inject certain malicious code to get the access of the administration and control the IoT system. Attackers can get the confidential data or delete the important data of the system. This attack at the application layer requires different mechanism than when the malicious attacks occur at lower layers.

2.9.3 Phishing Attack

The phishing attack is a kind of email attack; the authorized users lured to open the email and the attacker is hacking into the system to get the access control of the IoT system. The attackers may get the sensitive messages or confidential data to get control of the whole system. [11]

2.10 Application Layer Security

There are several security breaches can happen at this layer such as DDoS attack, malicious code injection attack and phishing attack.

2.10.1 Application Layer Security Services

The availability and non-denial of service protect the application layer from the distributed denial of service attacks. The anti-virus services protect the application layer from the malicious code injection attacks, and the anti-phishing services protect the application layer from the phishing attacks.

2.10.2 Application Layer Security Mechanisms

The availability and non-denial of service using IDS are needed at this layer to counter the distributed denial of service attacks. The anti-virus mechanism is required to counter the malicious code injection attacks, and the spam filtering mechanism [10] can counter the phishing attacks. In this chapter, we used the conception of security services and mechanisms as defined in ITU-T (X.800). ITU-T X.800 commends some security mechanisms to provide the security services defined in standards.

2.11 Standards and Protocols for IoT at Each Layer

Because a variety of networks, devices and applications exist in an IoT environment, a number of standards are used and different organizations. This makes the design complex and the implementation of a reliable IoT network even more complicated. IoT standards were only concerned with the IT industry in early 2013. As standards were later developed and implemented, IoT faced many security challenges and still has a long way to go from the universal IoT standard. In particular, IoT standards are not a standard " one fits all. " It's more like a pacemaker that fixes security issues and protects the IoT system against the threats of the attacker. Figure 6 shows the organizations and the different protocols currently used for IoT on each level.

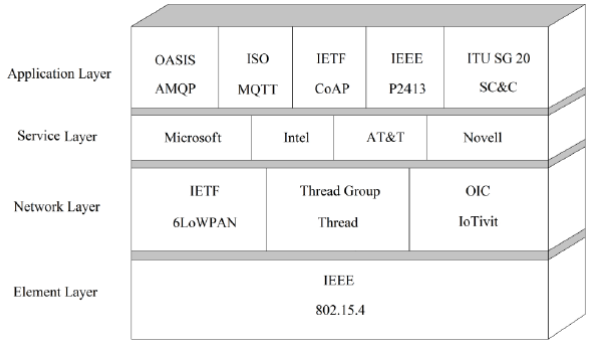

Figure 6: Organization and Protocols for IoT at Each Layer.

2.11.1 IEEE 802.15.4 at Element Layer

IEEE 802.15.4 is a standard specifying physical layer (PHY) and media access control (MAC) communication between devices in wireless personal area networks for low - cost communication. IEEE 802.15.4 implements and supports several security modes the advanced encryption standard (AES) symmetric cryptography mechanism;[11] these security modes provide security services such as confidentiality, authentication and integrity. Table 2 shows the IEEE 802.15.4 security services and security modes.

2.11.2 6LoWPAN at Network Layer

6LoWPAN is a network protocol that carries IPv6 packets in a low - powered IEEE802.15.4 wireless network environment. The 6LoWPAN implements the routing protocol (RPL) for the routing mechanism of low

power and loss networks (LLNs) and has three safety modes. The RPL implements the AES with 128-bit MAC keys and supports RSA with SHA-256 to ensure confidentiality and integrity for digital signatures. 12] Security modes are described below: unsecured: in this secure mode, the RPL sends data without any additional security, and this is the default RPL security mode. Preinstalled: By joining the RPL, the symmetrical keys will give the nodes. Authenticated: if a new device joins the network, the key authority authenticates the new device and authorizes it.
Preinstalled: By joining the RPL, the symmetrical keys will give the nodes. Authenticated: if a new device joins the network, the key authority authenticates the new device and authorizes it.

2.11.3 CoAP at Application Layer

The CoAP is running over the UDP. The UDP application layer reduces bandwidth requirements and supportsmulticast and unicast, and the CoAP targets resource-restricted devices such as mobile phones, tablets, laptops and low - power devices. The CoAP protocol provides a " demand and response " communication model between the endpoints and adopts the AES as the cryptographic algorithm for the provision of security services such as confidentiality, authentication and security. 2].[2]. Figure 7 shows the CoAP message header format. The CoAP header has 4 bytes which are: 2-bit version field, 2-bit message type, 4-bit token length, 8-bit code field and 16-bit message ID. The token enabled the CoAP to match the request and replies, the options define the format of the length value by specifying the option number according to its length and value.

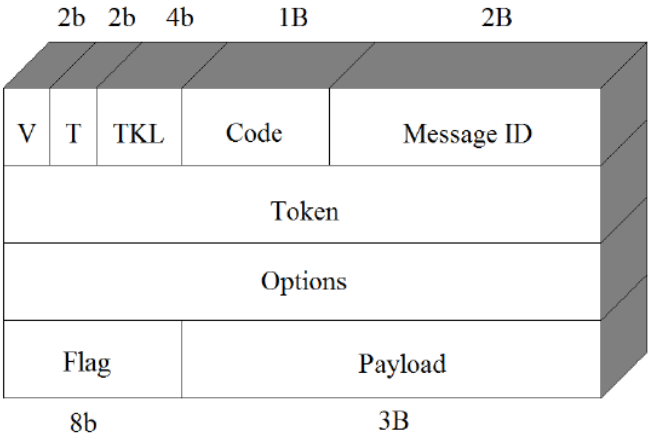

Figure 7: CoAP Message Header

III. IOT SECURITY LAYERED ARCHITECTURE

3.1 IoT Security Management System

The IoT security management system (IoTSMS) should be based on the IoT network system architecture. There are five fundamental security issues in the IoT network system, each of which should be considered in the security management system prior to design. These security problems are that intelligent sensors are easy to attack, security management should support low - power intelligent devices, element layer device privacy issues, different layers face similar threats, and system complexity and compatibility issues. These requirements mean that we need to develop a IoT security management system that addresses all perceived threats and is compatible with the architecture of the IoT network. In other words, since the IoT network environment is designed as a four - layer system architecture, it is perfectly appropriate to organize the network's security management in the same way as a layered architecture. In order to implement this concept, we propose a four - layer security management system for the IoT environment, similar to the IPSec functional architecture, as shown in Fig. 15. 4]. The proposed IoT security management system (IoTSMS) has four functional layers. The principles used to reach four layers are as follows: (i) A functionality layer is created where different types of security functions are required at different levels.
ii) Each layer carries out a well-defined safety function.
iii) The functionality of each layer is chosen taking into account the standardized protocols already in place.
iv) To minimize data flow across the system interfaces, the layer boundaries are selected.
v) The number of layers are compatible with the IoT system layers in such a way that distinct security functions need not be through in the same layer.

The security management system shown has three parts; on the left we have shown the architecture of the four - layer IoT network system. In the middle part, the IoTSMS has a four - tier management of security policy, IoT security services management, IoT security management mechanisms and IoT fundamental security functions. Such as pseudorandom generator, reverse multiplication, modular arithmetic, etc. Each layer has its

corresponding security management functionality to ensure confidentiality of data, data integrity and data access. On the right - hand side of this diagram is the IoT Security Management Information Base (SMIB), which implements the X.509 version 3 recommendation authentication to provide the conceptual data requirement segments of smart sensor IDs, user profiles, access control list and security logs.

3.2 Functional layers of Security Management for IoT

As mentioned earlier, there are four levels of IoT security management. They are the IoT security management policy layer, the IoT security management layer, the IoT security management mechanisms layer and the IoT basic security function layer. Each layer has a separate function to protect the IoT security system.

3.2.1 IoT Security Business Policy Management Requirements

The security policy management layer addresses the requirements of business users, such as preventing and detecting attacks from different attack points, protecting the privacy of all smart devices and protecting the IoT system against attacks and preventing system failures. Figure 8 shows the management of IoT security policy at minimum requirements.

4.2.2 IoT Security Services Function

The functional layer section of IoT security services provides the most common security services, such as authentication services, including peer-entity authentication and data origin authentication, confidentiality is probably the most common aspect of IoT security, including confidentiality of connections, connectionless confidentiality, selective field confidentiality and traffic flow privacy. Information in the IoT environment is constantly changing. Integrity services in this environment mean that only authorized entities and authorized mechanisms must make changes. Integrity services including connection integrity, connectionless integrity and selective field integrity; non-repudiation services including origin and destination non-repudiation services and access control services are essential to IoT system security. Figure 8 shows the functionality layer of IoT security services.

4.2.4 IoT Fundamental Security Function

A key feature of the IoT SMS is to be used as a comprehensive autonomous security server, which can simultaneously provide security for multiple applications. Therefore, the lowest layer of functionality includes a variety of general arithmetic and encryption modules. The basic safety function of IoT provides basic security functions such as single-way hash, message digest and secure hash algorithms. This layer includes key exchange security functions, including Diffie Hellman, elliptical curve and RSA algorithms. This layer may include digital signature and elliptical curve algorithms, authentication of messages, authentication code, time stamping and certificates including the X.509 certificate standard. This layer includes all the cryptographic elementary functions required to operate the IoT SMS. Figure 9 shows the basic security functionality layer of the IoT security modules

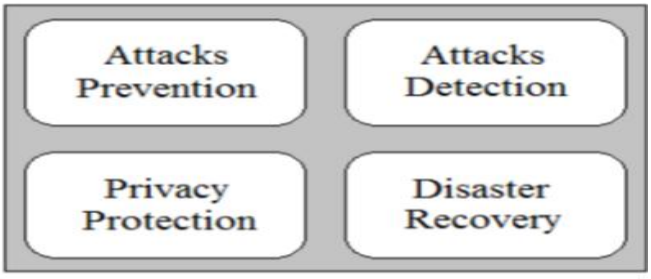

Figure 8. IoT Security Business Policy Management Requirements

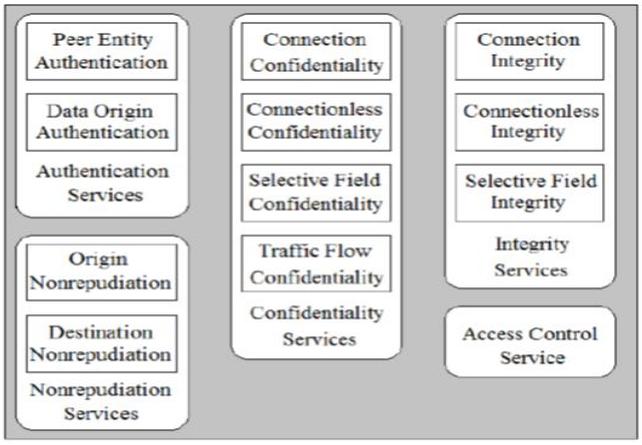

Figure 9. IoT Security Services Functionality Layer.

.

4.2.3 IoT Security Mechanism Function

Security mechanisms provide the necessary techniques, algorithms and schemes to support certain security services defined in the layer of security services. The layer of functionality of the IoT security mechanism provides the security mechanisms as either specific mechanisms or general mechanisms. Specific security mechanisms include encryption, digital signature, access control, data integrity, exchange of authentication, traffic padding, routing control and security notarization. Pervasive security mechanisms include trusted functionality, detection label, security audit trail, security recovery, network and host IDS and anti - virus security mechanisms. Figure 10 shows the layer of functionality of the IoT safety mechanism modules.

4.3 IoT Security Management Information Base

The IoT SMIB is a key component of the IoT text message. This database of information must be structured to support the implementation of all IoT security services in a computing or communication environment. The IoT security

management database is the concept segment of smart sensor IDs, user profiles, access control list and security logs. Note that this concept does not indicate any content or form for data storage. Figure 12 shows the segment of the IoT SMIB. As shown, the IoT SMIB is a repository of all the content information and parameters required to operate the IoT system normally. Interactions exist within and between IoT SMS and IoT SMIB layers.

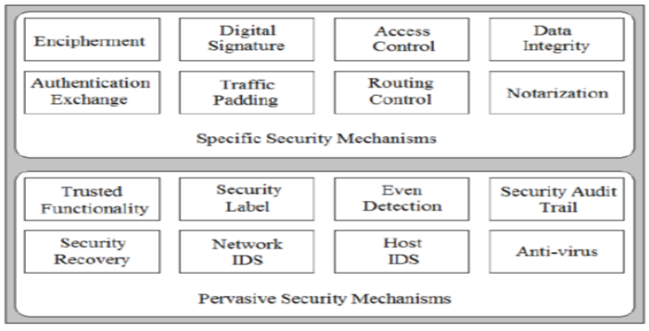

Figure 10. IoT Security Mechanisms Functionality Layer

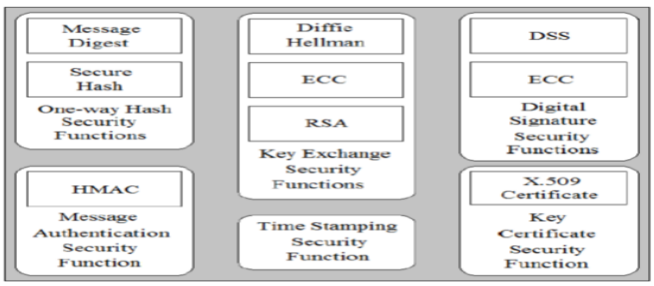

Figure 11. IoT Fundamental Security Functionality Layer.

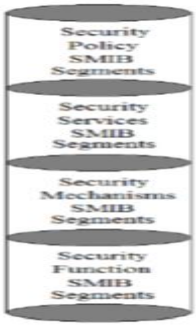

Figure 12. The IoT SMIB segments

4.4 PKI for the IoT Security

The Internet Engineering Task Force (IETF) has developed the Public Key Infrastructure (PKI) to offer a number of trust models. The important functions of PKI with regard to the security of the IoT system are the issuing of X.509 certificates, key storage and updating, the provision of services to a number of protocols and the provision of access control. The IoT system is not vulnerable to brute attacks and malicious attacks by having PKI in place. PKI ensures the integrity of the data collected by sensors and smart devices and provides protocol and application configuration access and availability. The PKI also ensures that the element layer is confidential in the IoT system.

Data are encrypted in the IoT system via the Wireless Sensor Network (WSN) nodes and transmitted to the gateway. The gateway decrypts the data and then encrypts the aggregated data to the top layers. According to conventional approaches, a key is secured between all sensors when the data collected is encrypted. The entire system is compromised if the key is compromised. PKI provides a pair of mathematically related public - private keys. If a key is used to encrypt data, the data can only be decrypted by the other key. In the case of the element layer in the IoT system, the data collected by the sensors and intelligent devices is encrypted using a public key and then decrypted using the private key.

4.5 Advantages of The Modular Security Management System for The IoT

The IoT security management system provides a modular structure that offers a multitude of security services and a multitude of safety mechanisms. The implementation of safety requirements for suppliers, network providers and manufacturers of devices. The different security service management module can invoke different security mechanisms by implementing the efficient basic security function to set optimum security and management requirements for the IoT network system. The modular security management system IoTSMS implements efficient security methods and systems in the IoT network system based on the security requirements of the users. The IoTSMS proposed can accommodate new security and new technologies and techniques. It provides a common security platform in an IoT system environment.

4.6 An IoT Security Management Scenario

Let us look at a smart scenario for home security management. The house owner wants to check the comfort level in his house. However, the owner of the house is at his / her place of work and wants to use his / her smartphone to monitor the temperature, humidity and illumination in his / her house.

4.7 Protocols Used In The IoTSMS Scenario

To illustrate the complexity of IoT security services, we go through a practical smart home scenario. We explain each function and the data for each layer. In order to meet the requirements of low - power and low-speed intelligent devices in the element layer, we should use the wireless communication protocol IEEE 802.15.4 to provide confidentiality, authentication and integrity with the necessary security services. At the network level, we need to use the LoPWAN protocol, which implements the routing mechanism for low power and loss networks. The routing mechanism implements AES with 128-bit MAC keys and supports RSA with SHA-256 for digital signatures to provide confidentiality and integrity security services. At the application level, we must use the CoAP protocol running across the UDP to reduce bandwidth requirements and support resource - constrained devices and low - power devices. The CoAP protocol provides a " demand and response " communication model between the endpoints and adopts the AES as the cryptographic algorithm for providing the security services mentioned above.

4.8 Data Flow of the Smart Home Scenario

If we consider the corresponding security service module, the security mechanism module and the basic security primitive module, we can determine the data flow in the smart home security management scenario.

1) The information on the environment, such as temperature, vapor concentration and light intensity, is collected by the various sensors. The data is then processed using a single-way hash function to create a digital signature message that is invoked in the element layer by the authentication service management module. The IEEE 802.15.4 protocol implements the AES symmetric key cryptography mechanism to encrypt data into 32-bit keys in CCM mode with message authentication and message integrity code

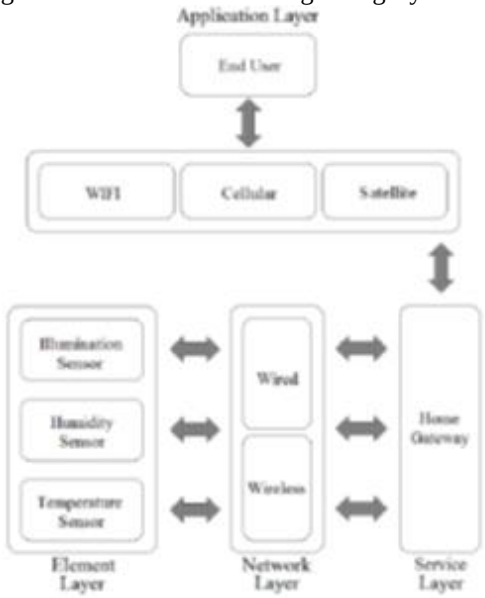

Figure 13. Concept of The Smart Home Scenario

2) Element layer data has been encrypted using the symmetric encryption function invoked by the network layer data integrity service management module. The 6LoWPAN protocol implements the routing mechanism for low - power and loss networks (RPL) that implements 128-bit keys for confidentiality and integrity security services in the AES.

3) The service layer received encrypted data and the Network Intrusion Detection System (NIDS) function module is used to prevent DoS attacks during transmission over the Internet, WIFI or cellular network.

4) The application layer authentication service management module invokes the key certification authority module to verify the user identity by comparing the user profile. The user then decodes the message using the PKI module's private key. The CoAP protocol provides a " request and response " communication model between the end points and uses the AES as a symmetric key cryptographic algorithm to provide confidentiality security services.

5) The user can now remotely monitor temperature, humidity and illumination in the house under efficient security protection using the Application Programming Interface (API) on the smartphone. Figure 13 shows the smart home scenario data flow. The chart shows the management of an IoT entity for the smart home scenario under consideration in each layer. The scenario above illustrates a simplified application. In the event of intruders and difficulties, there may be a number of possible problems that need to be solved. If the proposed IoTSMS is in place, this can be resolved easily.

IV. CONCLUSIONS

This study begins with a review of many case studies and IoT research designs. The IoT system is both a function and a state of the art design for the IT industry of today. Many research papers and academic journals focusing on the safety requirements of the IoT system have been published. None of them, however, pointed to a comprehensive safety management system in this context. The author's motivation for this research was the development of Google's automatic drive, wearable and health devices, virtual reality (VR) video games system and home network system. The first part of this research concerned the concept of safety in the IoT review of the literature in order to obtain the necessary background. The IoT is a new concept that is highly vulnerable to advanced cyber-attacks using Internet, telephone, mobile and satellite network systems. At first, the main focus was on understanding these attacks and their attack points in the IoT system. The second part of this research focused on the analysis and understanding of security and the IoT system techniques. In particular, the security

protocols, their components and entities required in each layer of the IoT system architecture were identified to analyze the vulnerabilities.

The third part of the study was to provide a comprehensive solution to the IoT system security problems. In this part of the study, a comprehensive autonomous security management system has been proposed that can provide security for several applications in the IoT environment at the same time. The IoT Security Management System (IoTSMS) is a layered functional architecture consisting of a number of entities or modules. The modular architecture of the IoTSMS enables all layers of the IoT system model to be secured against all potential threats and cyber-attacks. There are a number of proposals and patents relating to security systems and IoT security methods. To the knowledge of the author, however, most of them describe an incomplete and incomplete system for this purpose; in most cases they focus on a specific problem and provide a partial solution for a single part of the IoT system. The IoTSMS proposed in this study includes the steps to provide a plurality of mechanisms and to link services and mechanisms with a plurality of functions for security management.

This method supports all existing IoT protocols within the IoT system. The functional security architecture assumes four functional hierarchical layers along the same lines as the IoT system's hierarchical layer model and includes the IoTSMIB (security management information base) segment according to the four functional security layers. The implementation of this IoTSMS makes it easier to integrate new technologies and techniques.

REFERENCES

[1]. Ovidiu Vermesan, Peter Friess, Internet of Things: Converging Technologies for SmartEnvironments and Integrated Ecosystem. Aalborg, Denmark: River Publishers, 2013.

[2]. Punit Gupta, Jasmeet Chhabra, "IoT Based Smart Home Design Using Power and SecurityManagement," International Conference on Innovation and Challenges in Cyber Security,pp. 6-10, August 2016.

[3]. M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, "A Critical Analysis onthe Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications, vol. 111, pp. 1-4, February 2015.

[4]. Ovidiu Vermesan, Peter Friess, Internet of Things from Research and Innovation to MarketDeployment. Aalborg, Denmark: River Publishers, 2014.

[5]. Klaus Finkenzeller, RFID Handbook Fundamental and Applications in Contactless SmartCards, Radio Frequency Identification and Near-Field Communication. Wiltshire, UK: JohnWiley & Sons, 3rd ed., 2010.

[6]. Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "A Survey of Beacon-EnabledIEEE 802.15.4 MAC Protocol in Wireless Sensor Networks," IEEE Communication Survey & Tutorials, vol. 16, pp. 856-876, December 2013.

[7]. Saniya Vohra, Rohit Srivastava, "A Survey on Techniques for Securing 6LoWPAN," Fifth International Conference on Communication Systems and Network Technologies, pp. 643-646, April 2015.

[8]. Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez-Gallego, Jesus Alonso-Zarate, "A Survey on Application Layer Protocols for the Internet of Things," Transaction on IoT and Cloud Computing, pp. 1-8, April 2015.

[9]. Davide Conzon, Thomas Bolognesi, Paolo Brizzi, Antonio Lotito, Riccardo Tomasi,Maurizio A. Spirito, "An XMPP Based Architecture for Secure IoT Communications,"Interational Conference on Computer Communications and Networks, pp. 1-6, August 2012.

[10]. Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, "Internetof Things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10,pp.1497-1516, September 2012.

[11]. Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A Survey,"Computer Networks, vol. 54, pp. 2787-2805, October 2010.

[12]. Mr. Ravi Uttarkar and Prof. Raj Kulkarni, "Internet of Things: Architecture and Security,"International Journal of Computer Application, vol 3, pp. 12-19, June 2014.

Dr.P.Neelakantan". Security Issues in IOT"IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 12, 2018, pp. 81-93