Security on Internet of Things (IOT) with Challenges and Countermeasures

[1]R.Vignesh and [2]A.Samydurai
[1] Student, [2]Associate Professor
[1,2] Department of Computer Science and Engineering,
[1,2]Valliammai Engineering College SRM Nagar, Kattankulathur-603203, TamilNadu, India.

***Abstract* - This paper confers a survey and an investigates of the current status and analysis of Internet of things (IoT) security. The IoT structure pursue to append anyone with anything, anywhere. As against to the fixed Internet, in addition to humans, an IoT fastens a large number of machines, resource-coerced devices and sensors using different wired and wireless networks. An IoT normally has a three imaginary layers consisting of realization, Network, and Application layers. This paper narrates security problems within and across these layers. Many security ideas that should be implemented at each layer are also furnished. Previous work specific to enforcing security for each IoT layer and matching countermeasures are also reviewed. Finally, the paper presents future orientations for acquiring the IoT.**

Keywords - Confidentiality, availability, integrity, policies

---

1. Introduction

Internet of things (IoT) is gathering interconnected objects, services, people, and devices that can interact, share data, and information to attain goals in various areas and applications. IoT can be executed in many domains including transportation, agriculture, healthcare, energy production and distribution, and many other areas that require things to interact over the Internet to executes business assignments cleverly without human involvement. Devices joining in IoT typically follow an Identity Management (IM) approach to be identified in a group of comparable and different devices. A region in IoT can be defined by an IP address, however within that region each entity has a specific ID by which it is identified.

IoT approachess have seen rapid growth in recent years firstly publishing newer technologies like Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN). RFID qualifies the tagging or designating of every single device, so as to serve as the basic reorganization mechanism in IoT. Due to WSN, each "thing" (e.g., people, devices etc.) becomes a wireless distinguishable object that can interact among the physical, cyber, and digital worlds [1].

The rest of this paper is organized as follows. Section 2 describes the three-layer IoT structure and architecture. In Section 3, security problems relative to different security principles and the nature of IoT devices are presented. This section also contains the security problems interconnected with each layer of the IoT. Section IV discusses recent research works that aim to address the security issues in IoT by demonstrating countermeasures. Section 5 provides the big picture of all the security-related analysed work in IoT. Section 6 addresses the future orientations that can be taken in light of the current status of IoT security. Finally, the paper is concluded in Section 7.

2.Architecture

In an IoT architecture, each layer is explained by its functions and the devices that are used in the layer. There are different beleives regarding the number oflayers in IoT. However, according to many investigators [2-4], the IoT essentially utilizes on three layers which are the Perception, Network, and the Application layer. Each layer of IoT has intrinsic security issues related with it. Fig. 1 shows the basic three layer architectural strcuture of IoT with respect to the devices and technologies that surround each layer.

2.1. Perception Layer

The perception layer is also known as the"Sensors" layer in IoT. The motive of this layer is to receive data from the environment with the help of sensors. This layer observes, collects, and processes data from sensors and then convey it to the network layer. In addition, this layer may also performsIoT node combination in local and short range networks [3].

2.2. Network Layer

The network layer of IoT performs the task of data routing and communication to different IoT hubs and devices over the Internet. At this layer, Internet gateways, switching, and routing devices etc. run by using some of the very modern technologies such as WiFi, LTE, Bluetooth, 3G, Zigbee etc. to provide disperate network services. The network gateways serve as the negotiator between different IoT nodes by combining, filtering, and communicating data to and from different sensors [4].

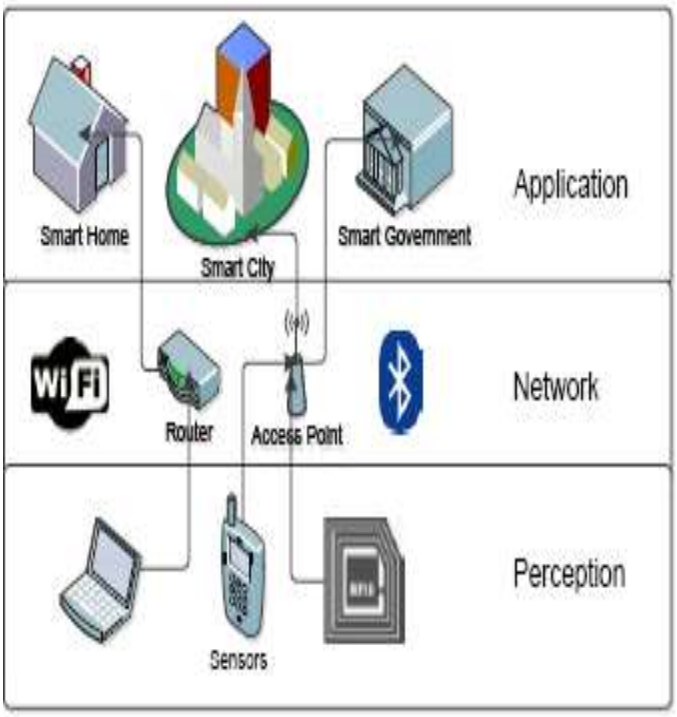

Figure 1. Three-layer IoT architecture

2.3. Application Layer

The application layer assures the authenticity, integrity, and confidentiality of the data. At this layer, the intention of IoT which is the creation of smart environments is executed.

3. security Issues in IoT

The same basic security objective of Confidentiality, Integrity and Availability that should be available for all interactions using computers and networks are needed to check the security of IoT. However, the IoT has many restrictions and limitations in terms of the components and devices, computational and power resources, and even the different and pervasive nature of IoT that introduce further studies to be addressed with respect to organising security. This section consists of two parts: the common security characteristics that the IoT must have, and the security problems peculiar to each layer of the IoT.

3.1.Security Features of IoT

The security challenges of IoT can be broadly divided into two classes; Technological and Security objection [5]. The technological challenges come due to the different and pervasive nature of IoT devices, while the security provocation is related to the ethics and usefulness that should be implemented to attain a secure network. Security should be included in IoT throughout the growth and running lifecycle of all IoT devices and hubs [4].Given below are the security principles that should be followed to achieve a secure interaction framework for the people, software, processes, and things in an IoT.

Confidentiality- It is important to ensure that data is secure and only available to approved users.
Integrity. The IoT is based on interchanging data and information between many various types of devices, which is why it is important to confirm accuracy of the data; that data is being comes from the right sender as well as to make sure that the data is not modified with during the process of transmitting due to intended or unintended interference.

Availability. The vision of IoT is to join as many smart devices as possible. The users of the IoT should have all the data visible whenever they need it. However data is not the only modules that is used in the IoT; devices and services must also be approachable and accessible when needed in a timely fashion in order to achieve the predictions of IoT.

Authentication-Each object in the IoT must be clever to clearly identify and authenticate other objects. However, this process can be testing because of the nature of the IoT; many entities are mixed up (devices, people, services, service providers and processing units). In addition, sometimes objects may need to communicate with other objects for the first time (objects they do not know) [8]. Because of all this, a methods to mutually authenticate entities in every communication in the IoT is required.

Lightweight Solutions-All of the security intentions considered earlier is not peculiar to IoT, although it may add special characteristics and constraints to each of them. However, in general confidentiality, integrity, availability and authentication are treated as basic intention in every computer or network security.

Figure 2. IoT security principles

Heterogeneity- The IoT connects different entities with contrasting potential, complexity, and vendors. The devices even have desperate dates and discharge versions, use desperate technical interfaces and bitrates, and are designed for an altogether different functions. Therefore obligations must be outlined to work in a variety of devices as well as in distinctive situations [2, 4, 8]. The IoT aims at connecting device to device, human to device, and human to human, thus it implements connection between different things and networks [5]. One more challenge that must be considered in IoT is that the environment is always changing (dynamics), at one time a device might be linked to a completely distinctive set of devices than in another time. And to ensure security optimal cryptography system is needed with an adequate key management and security protocols.

Policies-There must be policies and standards to ensure that data will be managed, protected, and transmitted in an efficient way, but more importantly a mechanism to accomplish such plan is needed to assure that every entity is implementing the standards. Service Level Agreements (SLO) must be clearly identified in every service involved. The enforcement of such guidelines will recommend trust by human users in the IoT model which will hereafter result in its growth and scalability.

3.1.8. Key Management Systems- In IoT, the devices and IoT sensors need to interchange some encryption materials to achieve confidentiality of the data. For this intention, there needs to be a lightweight key management system for all structures that can enable trust between different things, and can deliver keys by consuming devices' minimum capacity.

3.2. Security Threats in Each layer

Each IoT layer is manageable to security danger and attacks. These can be active, or passive, and can derive from external sources or internal network possess to an attack by the Insider [1]. The active attack through stops the service while the differential kind observes IoT network information without inhibit its service. At each layer, IoT devices and services are sensitive to Denial of Service attacks (DoS), which make the device, resource or network unavailable to approved users. The security problems at each layer are stated in Table 2, and given below is a brief examine of these problems with respect to each layer.

3.2.1. Perception Layer.

There are three security issues in IoT perception layer. First is the influence of wireless signals. Mostly the signals are sent between sensor nodes of IoT using wireless technologies whose effectiveness can be weaken by convulsing waves. Secondly, the sensor node in IoT devices can be attacked not only by the owner but also by the attackers because the IoT nodes usually run in external and outdoor environments, leading to physical attacks on IoT sensors and devices in which an attacker can tinkle the hardware components of the device. Third is the characteristic nature of network model which is dynamic as the IoT nodes are often moved around different places. The IoT perception layer mostly consists of sensors and RFIDs, due to which their storage kill, power utilization, and computation potential are very limited making them responsive to many kinds of dangers and attacks [1, 9].

The confidentiality of this layer can easily be abuse by Replay Attack which can be made by spoofing, modifying or replaying the identity information of one of the devices in IoT. Or the attacker might receive the encryption key by review the required time to perform the encryption what is known as Timing Attack. Another confidentiality dangering attack is when the attacker takes over the node and seizures all information and data which is basically Node Capture attack. Attacker can add another node to the network that threatens the integrity of the data in this layer by sending Malicious Data. This can also lead to a DoS attack, by consuming the energy of the nodes in the system and depriving it from the sleep mode that the nodes use to save the energy

[6].The above listed security issues at perception layer can be coped with by using encryption (which can be point-to-point or end-to-end), authentication (to verify true identity of sender) and access control [9]. Further security measures and protocols to address this issue are given in Section 4.

3.2.2. Network Layer.

As mentioned before, the network layer of IoT is also manageable to DoS attacks. Apart from the DoS attacks, the opponent can also attack the confidentiality and privacy at network layer by traffic examining, eavesdropping, and passive monitoring [1]. These attacks have a high likelihood of occurrence because of the remote access mechanisms and data interchange of devices. The network layer is highly manageable to Man-in-the-Middle attack, which can be followed by eavesdropping. If the keying material of the devices is eavesdropped, the secure interacting channel will be completely weakened. The key exchange mechanism in IoT must be secure enough to prevent any intruder from eavesdropping, and then accomplish identity theft.

3.2.3. Application Layer.

Since the IoT still does not have exhaustive policies and standards that supervise the communication and the enlargement of applications, there are many problems related to the security. Different software and applications have different authentication mechanisms, which makes unification of all of them very hard to guarantee data privacy and identity authentication. The large amounts of associated devices that share data will cause large elevated on applications that analyze the data, which can have big influence on the availability of the services.

4. IoT Security Remedies

IoT requires security computes at all three layers; at physical layer for data collection, at network layer for overpower and dispatch, and at application layer to maintain confidentiality, authentication, and integrity [4]. In this section the state-of-art security computes that address the specific characteristics and security intensions of IoT are discussed.

4.1. Authentication Measures

In 2011, Zhao et al. in [10] presented a change authentication strategy for IoT between platforms and terminal nodes. The strategy is based on hashing and characteristic extraction. The feature extraction was joined with the hash function to elude any collision attacks. This strategy actually assigns a good solution for authentication in IoT. The characteristics extraction process has the properties of irreversibility which is wanted to assure security and it is light weight which is helpful in IoT. The strategy focuses on authentication process when the platform is trying to send data to terminal nodes and not the opposite. while the strategy will improve the security while keeping the amount of information sent reduced, it works only on theory and there is no experimental proof of concept to support it.

Another method for ID authentication at sensor nodes of IoT is presented by Wen et al. in [9]. It is a one-time one cipher technique based on request-reply mechanism. Creating accurate access controls is as dominant as authentication for security, and these two usefulness go hand in hand in securing IoT. To address these functionalities, Mahalle et al. [5] presented an Identity Authentication and Capability based Access Control (IACAC) for the IoT.This research aims to fill the gap for an combined protocol with both authentication and access control accomplishment to attain mutual identity establishment in IoT. The model uses a public key approach and is consistent with the lightweight, mobile, distributed, and computationally limited nature of IoT devices plus existing access technologies like Bluetooth, 4G, WiMax, and Wi-Fi. It prevents man-in-the-middle attacks by using a timestamp in the authentication message between the devices, which serves as the Message Authentication Code (MAC).

The strategy works in three stages; first a secret key is generated based on Elliptical Curve Cryptography-Diffie Hellman algorithm (ECCDH) [11], then identity construction is made by one-way and mutual authentication protocols, and lastly access control is implemented. The shared secret key is initiated by the combination of public key and a private parameter, and has small size and low computational overhead due to the use of Elliptic curve cryptography (ECC). The entry is allowed by storing a experts with access rights, device identifier, and a random number in each IoT device. This random number is the result of hashing device ID with access rights. The IACAC model does not perfectly prevent DoS attacks. However, it decreases it since entry of resource is granted to only one ID at a time.

4.2. Trust Establishment

Since, the things or devices in IoT can physically move from under one owner to a heterogeneous one, trust should be accepted between both owners to starts a smooth transition of the IoT device with respect to access control and permissions. The work in [13] presents the opinion of common belief for inter-system security in IoT by creating an item-level access-control framework. It constructs trust from the creation to operation and dispatch phase of IoT. This trust is established by two mechanisms; the creation key and the token.

4.3. Mediated Architecture

Not having common strategies and standards to control the design and the execution of algorithms in IoT makes it hard to control the security. It is major for IoT to have a merged architecture that supports internal autonomy or a centralized unit to overcome the heterogeneity of various devices, softwares and protocols. The work in [14] recommended a clarification for combined IoT, and based on that definition an access control delegation model is presented. The presented model takes into consideration the flexibility and scalability that are key characteristics in IoT systems. Another such seek was made in [15] to propose a framework called Secure Mediation GateWay (SMGW) for critical infrastructures. This addresses an speculation of IoT as it is applicable for any kind of distributed infrastructures that are completely heterogenous in their nature and operation. SMGW can recognize all the appropriate allocate information from different nodes, and can overcome the heterogeneity of heterogeneous nodes whether it is a telecommunication, electrical, water distribution node, and can interchange all the messages and information over the untrusted network of Internet. This work qualifies the follow-up of another federated approach, presented in [4] to provide the structure of Smart Home based on the SMGW.

It is not enough to have procedures and standards to assure security, mechanisms to enforce such procedures are also needed. The research by Neisse et al. in [16] addresses this problem by combining a security toolkit named SecKit with the MQ Telemetry Transport (MQTT) protocol. The current procedures may not be effective in IoT because of its dynamic nature. The proposed procedure mechanism can have good impact in assuring the security of the IoT, however it introduced additional delay in the process.

4.4. Security Awareness

Another key security computes for the success and growth of IoT structure is the awareness and review among human users which are a part of IoT network. In [17] the authors described the outcome of not securing the IoT using actual numbers. They a IoT devices (SCADA devices, web cameras, traffic control devices, and printers) that were publicly obtainable using either no-password or the default password. The collected results were very interesting and showed that many of these devices were actually attainable. If people continued with the same unawareness towards security, and used the least amount of security like normal password that comes with the product, this would make the IoT to cause more mischief than good. Hackers will gain more occasions to conduct attacks against the whole network if one of its devices is not secured.

5. The overview Picture

IoT security is insistent by the many factors and security integrities discussed earlier, and the problems that are faced by IoT security has been the focus of many researchers for long time. In this section, an evaluation of some related work is furnished and the offerings of this paper are given. In survey paper presented by Roman et al. in [7], a detailed introduction about the IoT and security problems alongwith the need to have IoT standards are explained. However, no remedies are provided for the given security threats. This work was followed by the survey resolution in [8] in which remedies are provided for all security threats.

6. Future Directions

IoT has seen rapid improvement in recent years in the areas of telemedicine platforms, intelligent transportation systems, logistics observing, and pollution observing systems etc. Some examiner even believes that the number of things combined will increase up to 26 billion units by 2020 [4]. However, the security threats related to the IoT must be dealt with to its growth and maturation. Given below are coming directions for research in order to make the IoT more protection.

6.1. Architecture Standards

IoT currently employs different devices, services, and obligations to achieve a common intention. However, to accommodate a network of IoT structures to achieve a bigger structure, for example, to form a smart town by the combining of many smart homes, there needs to be a set of rules that should be followed from the micro to macro levels of IoT recognization. The present day requirement of IoT is to have well-specified architecture standards comprising of data models, interfaces, and obligations that can support a wide range of humans, devices, languages, and operating system.

6.2. Identity Management

The identity management in IoT is performed by interchanging finding information between the things for first time connection. This process is affected to overhear which can lead to man-in-the-middle attack, and thus can threaten the whole IoT structure. Hence, there needs to be some pre-defined identity management entity or hub which can observes the relation process of devices by applying cryptography and other techniques to prevent identity theft.

6.3. Session layer

As per most of the researchers, the three-layer architecture of IoT does not contain the opening, closing, and governing a session between two things. So, there is a need for obligations which can address these problems and can simple the interaction between devices. An abstract session layer should be containas an additional layer in IoT architecture which can specifically govern the connections, obligations, and sessions between communicating different devices.

6.4. 5G Protocol

To realize the execution of IoT, IPv4 will definitely fall short in containing the huge numbers of IP-identifiable objects. That is the reason why there is a move towards executing IPv6, which is able to support 3.4x1038 devices. However, such large number of devices will create a large amount of traffic, which can lead to more delays and thus more bandwidth will be required. The intention of the new generation of communication (5G) is to provide speed between 10-800Gbps, differentiating this number with the current technology (4G) with speed of 2-1000 Mbps, 5G should be able to grasp the traffic produced by IoT devices. 5G technology is also expected to accommodate both IPv4 and IPv6 by using IPv4/IPv6 structure translation

7. Conclusion

The IoT framework is vulnearble to attacks at each layer. Therefore, there are many security threats and requirements that need to be dispatched. Current state of research in IoT is mainly concentrated on authentication and access control protocols, but with the rapid growth of technology it is essential to consolidate new networking protocols like IPv6 and 5G to achieve the progressive mash up of IoT topology.

The major developments supported in IoT are mainly on small scale including within companies and in some limited industries. To scale the IoT structure from one company to a discipline of different companies and different systems, various security interests need to be addressed. The IoT has great likely to transform the way we live today. But, the foremost discipline in recognization of completely smart structures is security. If security disciplines like privacy, confidentiality, authentication, access control, end-to-end security, trust management, global policies and standards are consigned completely, then a transformation of everything by IoT can be realised in the near future. There is need for new identification, wireless, software, and hardware technologies to resolve the currently open research threats in IoT like the standards for different devices, implementation of key management and identity establishment systems, and trust management hubs.

8. References

[1]M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.

[2]K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[3]L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network
characterization," Computer Networks, vol. 56, 3594-3608, 2012.

[4]M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

[5]P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[6]M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.

[7]R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, 51-58, 2011.

[8]R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.

[9]Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in Int'l Conference on Cloud Computing and Intelligent Systems (CCIS), 1062-1066, 2012.

[10]G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in Int'l Conference on Modelling, Identification and Control (ICMIC), 563-566, 2011.

[11]N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48, 203-209, 1987.

[12]J.-Y. Lee, W.-C.Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Int'l Symposium on Next-Generation Electronics (ISNE), 1-2, 2014.

[13]Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014.

[14]B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in Int'l Symposium on Wireless Personal Multimedia Communications (WPMC), 604-608, 2012.

[15]M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," Int'l Journal of Critical Infrastructure Protection, vol. 5, 86-97, 2012.

[16]R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 165-172, 2014.