International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

A COMPREHENSIVE ANALYSIS OF SECURITY REQUIREMENTS AND APPROACHES FOR INTERNET OF THINGS

Mrs. Divya Sharma, Assistant Professor, Department of ECE, New Horizon College Of Engineering, Bangalore ;
Mrs. Ishani Mishra, Assistant Professor, Department of ECE, New Horizon College Of Engineering, Bangalore;
Dr. Sanjay Jain, HOD- Department of ECE, New Horizon College Of Engineering, Bangalore

Abstract

The Internet of Things (IoT) is a concept that has become more popular lately, wherein everything real becomes virtual, which means that each person and thing has a locatable, addressable, and readable counterpart on the Internet. With these characteristics, the IoT promises to extend "anywhere, anyhow, anytime" computing to "anything, anyone, any service." However, several significant barriers exists to fulfil the IoT vision, one of them being security. The Internet and its users are already under continual attack, where the invaders have taken advantage of the present foundational weaknesses. Therefore, without strong security measures, attacks and malfunctions in the IoT will outweigh any of its benefits. To establish a secured environment for any IoT application we need to understand the IoT conceptually, evaluate Internet security's current state, and expore how to move from solutions that meet current requirements and constraints to those that can reasonably assure a secure IoT. In this paper we discuss the security challenges and its requirements with respect to the different layers of an IoT architecture. Further we have extended our study to classify the security measures to be implemented at each layer.

KEYWORDS: Internet of Things (IoT), layered security requirements, layered security methods.

1. Introduction

We have already stepped into the world of smart devices such as Smartphones, Smart cars, Smart homes, Smart cities thereby making the world smart [1]. Examples of such are temperature sensors, humidity sensors or even the luminosity sensor in a mobile phone. Due to the vast amount of sensors that exist, the amount of data that get produced every second is mind-boggling and it would seem difficult to organize it all in a good and easy way. There have been many attempts to create systems that allow users to register their sensors and view the produced data. This has led to evolution of the IoT-Framework, in an effort to easily view, handle and interact with data streams.

Within the system, users can register their sensors, create streams of data , and view them on a graph.

IoT definitely has a great potential for flexibility and promises a great future . Still there are several issues to be considered for its wide adoption and without resolving them we cannot expect a successful IoT.

In this paper we have taken into account the issues concerning the security of an IoT. Due to easy accessibility of the objects, it can be easily exploited by the evil-minded hackers [2]. Since the devices have a direct impact on the lives of users so security considerations must be a high priority and there must be some proper well-defined security infrastructure with new systems and protocols that can limit the possible threats related to scalability, availability and security of IoT [3].

The paper is organized as follows. Section 1 describes about the security requirements in IoT. Section 2 describes the layered security issues. Section 3 discusses the required security methods in each layer.

2. IoT Network Security Requirements

IoT must have strong security foundations built on a holistic view of security for all IoT elements at all stages—from the identification of objects to the provisioning of services, from the acquisition of data to the governance of the whole infrastructure [4]. All security mechanisms must consider each object's lifecycle and services from the very beginning of that object's existence. In this section, we have discussed the major security objectives in IoT :

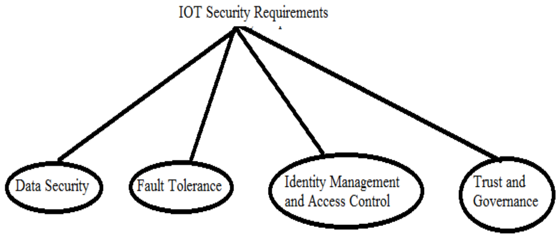
IOT Security Requirements
Data Security
Fault Tolerance
Identity Management and Access Control
Trust and Governance

Figure 1. Security Requirements in IoT

i) **Data Security**: Data security has three main objectives:

Data Confidentiality: Messages that flow between a source and a destination could be easily intercepted by an attacker and secret contents are revealed. Therefore, these messages should be hidden from the intermediate entities; in other words, End-to-End (E2E) message secrecy is required in the IoT. Also, the stored data inside an IoT device should be hidden from unauthorized entities [6].

Data Integrity : No intermediary between a source and a destination should be able to undetectably change secret contents of messages, for example a medical data of a patient. Also, stored data should not be undetectably modified.

Data Availability: For smooth working of the IoT and access to data whenever needed, it is also important that services that applications offer should be always available and work properly. In other words, intrusions and malicious activities should be detected.

ii) **Identity Management and Access Control:** Proving identity is an important part of identity management. As developers create a worldwide network of objects, they must build an infrastructure that allows mutual object authentication. There must be a balance between centralized management and a distributed, hierarchical approach. Illegal access to device and data will put the security of the network at stake. Access control methods must be incorporated to prevent loss of overall security system.

iii) **Trust and Governance**: Trust is an essential security component in IoT deployment. In IoT incorporating trust will not only reduce uncertainty among objects as they interact but also encompass how users feel while interacting in the IoT. Feelings of helplessness and being under some unknown external control can greatly undermine the deployment of IoT-based applications and services. Users must be able to control their own services, and they must have tools that accurately describe all their interactions so that they can form an accurate mental map of their virtual surroundings.

Governance helps strengthen trust in the IoT. A common framework for security policies will support interoperability and ensure security's continuity. In the IoT, such mechanisms must be able to define trust in a dynamic, collaborative environment and understand what it means to provide trust throughout an interaction.

iv) **Fault Tolerance**: IoT will be more susceptible to attack than the current Internet. Fault tolerance is indispensable to assure service reliability. Objects should be able to defend themselves against network failures and attacks. The advent of new IoT networks and applications has also provided attackers a new platform to be exploited. Several new threats have been reported which aim at disrupting the network security to greater extent. Thus, existing cryptographic techniques will fail in safeguarding the network in all aspects.

3. Layered Security Challenges

There have been many achievements in the research field of IoT, however there are still some open challenges that needs to be addressed for the ubiquity of this technology [5]. Figure 2. Shows the layered architecture of an IoT network. In this section we examine the various challenges faced in developing security control methods at each architectural layer.

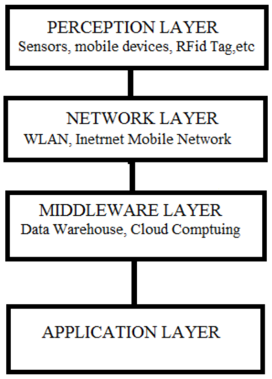
PERCEPTION LAYER
Sensors, mobile devices, RFid Tag,etc
NETWORK LAYER
WLAN, Inetrnet Mobile Network
MIDDLEWARE LAYER
Data Warehouse, Cloud Comptuing
APPLICATION LAYER

Figure 2. Architecture Layers of IoT

3.1 Perception Layer:

This layer consists of different kinds of IoT devices. These devices are heterogeneous, tiny wirelessly connected resource-constrained nodes. Example of such devices would be sensor nodes, RFid tags, handheld devices like mobile phones etc. These devices are expected to have varied characteristics depending upon the area of application. The IoT's highly distributed nature and use of fragile technologies, such as minimal capacity embedded devices in public areas, create weak links thereby making it an easy target to vulnerabilities. Easily accessible objects in unprotected zones, such as city streets, are prone to physical harm. Like compromising botnets, some objects would try to hinder services from the inside.

Securing theses IoT devices is challenging due to following reasons:

Heterogeneity: Heterogeneous devices (sensors RFID tags,etc), mobile devices(cars,mobile phones,etc) are interconnected which demands for different security techniques.

Resource Constrained Devices: Some IoT devices, such as passive RFID tags, might be extremely constrained. Cryptographic mechanisms must be smaller and faster but with little or no reduction in security level. IoT extensively uses Internet standards for communication and service provision. Still, some devices, such as sensors like the one used to check the state of runway lights, will lack the resources to implement the Internet security mechanisms that normally protect these kinds of interactions. Therefore, security protocols require some forward-looking adaptation. Subtle differences between IoT and Internet protocols might lead to gaps in end-to-end security. Further, adaptations should not only fulfill the IoT's performance requirements but also provide the protocol's original security properties in the context of the Internet architecture.

Massive Scaling: The current trajectory of the numbers of smart devices being deployed implies that eventually trillions of things will be on the Internet. How to name, authenticate access and protect such a large scale of things are major problems.

3.2 Network Layer:

The purpose of this layer is to transmit the gathered information obtained from the physical layer, to any particular information processing system through existing communication networks like Internet, mobile Network or any other kind of reliable network.
The main challenge in framing network security algorithms is due to following reason: *Openness of the system:* For example cars are automatically transmitting maintenance information and airplanes are sending real-time jet engine information to manufacturers. There is or will be even greater cooperation and 2-way control on a wide scale: cars (and aircraft) talking to each other and controlling each other to avoid collisions, humans exchanging data automatically when they meet and this possibly affecting their next actions, and physiological data uploaded to doctors in real-time with real-time feedback from the doctor. These systems require openness to achieve these benefits. Of course, openness will cause difficulty with security and privacy. Thus we need to ensure that openness provides a correct balance between access to functionality and security and privacy.

3.3 Middle-ware Layer:

This layer is composed of data storage technologies like cloud computing. This layer includes information processing systems that take automated actions based on the results of processed data and links the system with the database which provides storage capabilities to the collected data. This layer is service-oriented which ensures same service type between the connected devices. It also provides different interfaces for the applications and data storage facilities. The major security issue arises due to following reason:
Big Data: The amount of collected data will be enormous. It can be expected that a very large number of real-time sensor data streams will exist, that it will be common for a given stream of data to be used in many different ways for many different inference purposes, that the data provenance and how it was processed must be known because any uncertainty in interpreted data can easily cause users not to trust the system.
Therefore Trust is one important aspect of the usefulness of big data. Security and privacy are essential elements of trust.

3.4 Application Layer

This layer realizes various practical applications of IoT based on the needs of users and different kinds of industries such as Smart Home, Smart Environment, Smart Transportation and Smart Hospital etc.
These applications can be corrupted by the attackers to disrupt the IoT system. Security techniques need to be implemented for efficient functioning of the application.

4. Layered Security Methods in IoT

Research is being done to provide a reliable well-defined security architecture which can provide confidentiality of the data security and privacy [5]. Also, attempts are being made to make the system resilient to various attacks. In this section, possible security methods that can be incorporated at each layer have been explained.

4.1 At Perception Layer

4.1.1 Hash Algorithms:

Hash Algorithms are used for authentication. These algorithms provide digital signatures to the terminals that could withstand all the possible known attacks like Side-channel attack, Brute force attack and Collision attack etc.

4.1.2 Encryption Techniques:

Privacy of the data at perception layer can be ensured by enforcing symmetric and asymmetric encryption algorithms such as RSA, DSA, BLOWFISH and DES etc which prevents an unauthorized access to the sensor data while being collected or forwarded to the next layer.
However, the devices to be protected are constrained in resources, but attackers are not. So we need to

implement the encryption algorithms in a lightweight manner. The modified encryption algorithms should be lightweight in resource consuming, but NOT in security weight. The cryptographic community is emerging with a great deal of specialized lightweight cryptographic algorithms, which include stream ciphers like PRINCE [7], PRESENT [8], CLEFIA [9] to mention few of them.

4.1.3. Intrusion Detection Mechanism:

Any unauthorized entity gaining access to device must be immediately reported. Illegal access to the devices must be prevented by enabling efficient Intrusion Detection systems.

4.2 At Network Layer :

4.2.1 P2P Encryption:

With the help of a proper authentication process and point to point encryption, illegal access to the devices to spread fake information could be prevented. The most common kind of attack is the DoS attack which impacts the network by driving a lot of useless traffic towards it through a number of botnets fueled by the system of interconnected devices. Also distribution of the keys should be done in a secure manner.

4.2.2 Routing Security:

Even with the communication security that protects the messages with confidentiality and integrity services, a number of attacks are possible against networks mainly to breach availability security services. These attacks aim to disrupt networks by interrupting, for example, the routing topology or by launching DoS attacks. By implementing security aware routing protocols, we can find secured path to transmit data. Even through secured routing approaches we can detect any malicious nodes or botnets present in the network.

4.2.3 Intrusion Detection Systems (IDS):

Effective IDS mechanisms are required to detect impostors and malicious activities in the network, and firewalls are necessary to block unauthorized access to networks.

4.3 At Middleware and Application Layers:

4.3.1 Integrated Identity Identification:

Authentication process at these layers is done using integrated identity identifications to prevent the access by any miscreant user. How the data was created and who created it must be validated using digital signatures etc.

4.3.2 Intrusion Detection Mechanism:

At middleware layer intrusion detection techniques focus on providing solutions for various security threats by generating an alarm on occurrence of any suspicious activity in the system due to the continuous monitoring and keeping a log of the intruder's activities which could help to trace the intruder. There are different existing intrusion detection techniques [10] including the data mining approach and anomaly detection.

4.3.3 Risk Assessment:

After implementing security controls risk assessment must be done using tools. It will give justification for the effective security strategies and provides improvements in the existing security structure.

4.3.4 Encryption Techniques:

Data security is ensured by various encryption technologies which prevent the data stealing threats. Two primary considerations when choosing the cryptographic suite to use for protecting information are level and performance. Elliptic curve cryptography provides strong algorithms yet small key sizes for Encryption key establishment and Digital Signatures. When paired with a symmetric algorithm such as Advanced Encryption Standard (AES), this cryptographic suite offers strong data protections. Moreover, to prevent other malicious activities from the miscreant users, Anti- Dos firewalls and up to date spywares and malwares are introduced.

5. Conclusion

Security at all the levels of IoT is expository to the functioning of IoT. Recently, several solutions have been proposed for effective implementation of a security infrastructure for IoT. However, these achievements need to be further expanded to be applicable in various IoT domains.

In this paper the security issues, requirements and security methods for IoT architecture have been presented. In the future, more authentications, risk assessment and intrusion detection techniques in each architectural layer must be explored. Also both proactive and reactive solutions must be provided to make the system resilient to attacks. In proactive approaches the attackers will find it difficult to break the security via the attacks whereas in reactive approaches once the attack occurs the system must be able to recover from them.

Further, legal frameworks, proper regulations and policies must be devised to ensure stable development of the secure technologies.

References

[1] Shi Yan-rong, Hou Tao, Internet of Things key technologies and architectures research in information processing in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013.

[2] Rodrigo Roman, Pablo Najera and Javier Lopez, ”Securing the Internet of Things,” in IEEE Computer, Volume 44, Number 9, 2011, pp. 51-58.

[3] Friedemann Mattern and Christian Floerkemeier, ”From the Internet of Computers to the Internet of Things,” in Lecture Notes In Computer Science (LNCS), Volume 6462, 2010, pp 242-259.

[4] “Securing the Internet of Things” Article published in IEEE Computer, vol. 44, no. 9, pp. 51-58, September 2011, Rodrigo Roman, Pablo Najera, and Javier Lopez University of Malaga, Spain.

[5] “A Critical Analysis on the Security Concerns of Internet of Things (IoT), “International Journal of Computer Applications (0975 8887)Volume 111 - No. 7, February 2015.

[6] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, ”Internet of Things: Vision, applications and research challenges,” in Ad Hoc Networks, 2012, pp.1497-1516 Luigi Atzori, Antonio Iera, Giacomo Morabito, ”The Internet of Things: A Survey,” in Computer Networks, pp. 2787-2805..

[7] “PRINCE A Low-latency Block Cipher for Pervasive Computing Applications”, Julia Borgho, Anne Canteaut, Tim Guneysu, Elif Bilge Kavun, Miroslav Knezevic.

[8] PRESENT: An Ultra-Lightweight Block Cipher A. Bogdanov, L.R. Knudsen, G. Leander , C. Paar1, A. Poschmann1, M.J.B. Robshaw, Y. Seurin, and C. Vikkelso.

[9] “The 128-bit Blockcipher CLEFIA” Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai1, and Tetsu Iwata Sony Corporation.

[10] Animesh Patcha, Jung-Min Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, in Computer Networks, Volume 51, Issue 2, 2007.

Acknowledgments

The authors are thankful to IJACT Journal for the support to develop this document.