A Survey On Data Security In IoT

Mercy Milcah Y[1], Mohanapriya K[2], Moorthi K[3]
Department of Computer Science Engineering
[1,2,3] Jansons Institute of Technology, Tamil Nadu

Abstract- *An auspicious technology of Internet of things is becoming more familiar than ever, as it increases the level of communication along with the increasing population. Internet of Things (IoT), aims at connecting through the internet, quite a number of devices we use on daily basis, effectively merging the physical and digital worlds, leading to a new era of internet. Through IoT, billions of devices are able to share data and communicate over the internet without humans involved, making the devices digitally intelligent. As the data increases every day, threats for the security of those data also multiply, with increasing issues faced by the devices that are challenging. In this paper, we have put forward a survey on various security issues that is faced by the data being shared by the devices through the technology of Internet of Things (IoT).*

Keywords- Internet of Things (IoT), Security issues, Challenges

I. INTRODUCTION

Data security has been an issue ever since the first two computers were connected to each other. As internet became a profit-oriented system, security concerns also expanded to cover personal privacy, financial transactions, and the threat of cyber-theft. In IoT, security is inseparable from safety, after a number of high-profile incidents where a common IoT device was used to infiltrate and attack the larger network. Implementing security measures is critical to ensure the safety of networks with IoT devices connected to them.

IoT has become an inseparable part in every aspect of our personal lives. Though it is a part of the beauty and enchantment of modern technological advancement, it is also a pause for concern when it is down to data sharing and potential security breaches. Considering the microchip, a remarkable example of the need for IoT data security and privacy, the potential for risk begins at a far more basic level. Even the most simple and seemingly harmless household devices gather deeply personal data about users' day-to-day lives. While such opportunities for data collection might seem obvious to those in the tech industry, many consumers, content with the ease and convenience of IoT, don't realize the extent to which their personal data is analyzed and used.

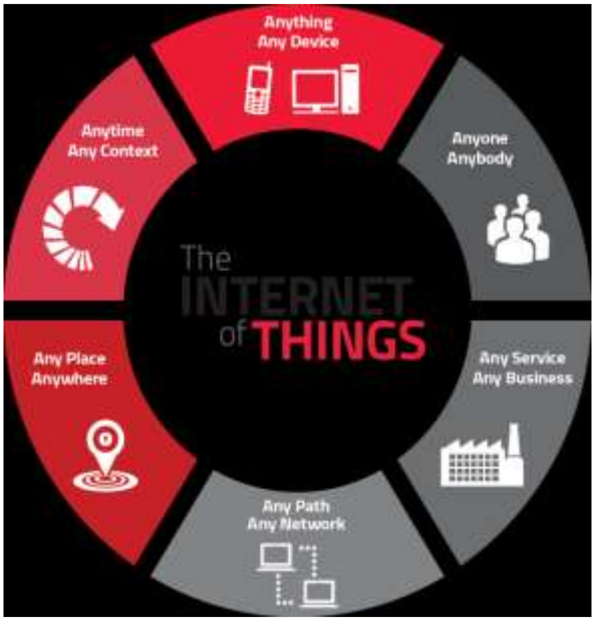

Fig .1. Internet of Things (IoT)

Applying existing Internet standards to smart devices can simplify the integration of the envisioned scenarios in the IoT contexts. However, the security mechanisms in conventional Internet protocols need to be modified or extended to support the IoT applications. We can list the threats of IoT under three categories; Privacy, Security and Safety. Experts say the security threats of the Internet of Things are broad and potentially even crippling to systems. Since the IoT will have critical infrastructure components, it presents a good target for national and industrial surveillance, as well as denial of service and other attacks. Another major area of concern is privacy with the personal information that will potentially reside on networks, also a likely target for cyber criminals. Then, we will review the recently proposed IoT authentication schemes and architectures.

II. LITERATURE REVIEW

A. IoT security issues

A review [1], by Mudassar Ahmad et al, presents analysis and survey on IOT security, also discusses the current status and challenges of IOT security. Typically, there are three layers in IoT architecture (Fig.2), i.e. perception layer, network layer, and application layer. For secure internet of things realization, at each layer a number of security principles should be enforced. Their study also provides an overview on proposed countermeasures and challenges of Security. Each layer of IoT is susceptible to attacks; therefore, there is need to address security challenges and requirements of IoT framework. For the dynamic mashup of internet of things topology, in the future there is need of new protocols for networking like ipv6 and 5G.

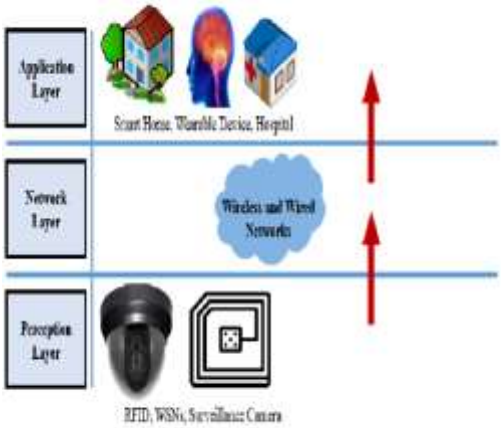
Application Layer
Smart Home, Wearable Device, Hospital
Network Layer
Wireless and Wired Networks
Perception Layer
RFID, WSNs, Surveillance Camera

Fig .2. Security in IoT Architecture Layers

This paper [8], by Mirza Abdur Razzaq et al, presents an extensive comprehensive study on security and privacy issues in IoT networks. Due to lack of security mechanism in IoT devices, many become soft targets and even without the victim’s knowledge of being infected. In their paper, the security requirements are discussed such as confidentiality, integrity, and authentication, etc. Twelve different types of attacks are categorized as low-level attacks, medium-level attacks, high-level attacks, and extremely high-level attacks along with their nature/behavior as well as suggested solutions to encounter these attacks are discussed.

Suchitra.C and Vandana C.P proposed a paper [9] where, they analyzed the various security requirements and challenges in IoT and research objectives and discussed the current state of internet of things and analyzed the various security issues in IoT. They briefed the communication protocol stack employed in IoT and various layered in IoT architecture. In future, a framework to detect Denial of Service (DoS) attack in IoT will be proposed and its effectiveness will be measured.

In this paper [10] by Ajish K S et al, a study of IoT being the interconnection of various physical devices, security between these connected devices is a major concern, due to the rise of cyber-attacks, and the rise of black hats, security of users connected are a major concern. Their paper is the survey of all these situations, where they bring in the insight of security issues of some of the common and major hardware devices used in IoT devices such as RFID systems, Beacon and Raspberry Pi.

Engin Leloglu, the author of a review [15], defines security requirements and challenges that are common in IoT implementations and discusses security threats and related solutions on each layer of IoT architecture to make this technology secure and more widespread accordingly.

i) Interoperability: Relevant security solutions should not prevent the functionality of interconnected heterogeneous devices in IoT network system.

ii) Resource constraints: In IoT architecture, most of nodes lack of storage capacity, power and CPU. They generally use low-bandwidth communication channels. Hence, it is unable to apply some security techniques such as frequency hopping communication and public key encryption algorithm. Setup of security system is very difficult under these circumstances [6].

iii) Data volumes: Although some IoT applications use brief and infrequent communication channels, there are considerable number of IoT system such as sensor-based, logistics and large scale system that have potentials to entail huge volume of data on central network or servers.

iv) Privacy protection: Since a great number of RFID systems are short of suitable authentication mechanism, anyone can tracks tags and find the identity of the objects carrying them. Intruders can not only read the data, but can also modify or even delete data as well .

v) Scalability: The IoT network consists of a large number of nodes. The proposed security mechanism on IoT should be scalable [9].

vi) Autonomic control: Traditional computers need users to configure and adapt them to different application domains and different communication environments. However, objects in IoT network should establish connections spontaneously, and organize/ configure themselves for adapting to the platform they are operating in. This kind of control also involves some techniques and mechanisms such as self-configuring, self-optimizing, self-management, self-healing and self-protecting.

B. Security and Privacy

Mehiar Dabbagh and Ammar Rayes [3] put forward the IoT security challenges and IoT security requirements. Three-domain IoT architecture was considered in our analysis where we analyzed the attacks targeting the cloud domain, the fog domain, and the sensing domain. Our analysis describes how the different attacks at each domain work and what defensive countermeasures can be applied to prevent, detect, or mitigate those attacks.

This paper [12] proposed by Djamel Eddine Kouicema , Abdelmadjid Bouabdallaha and Hicham Lakhlefa where they provide a comprehensive top down survey of the most recent proposed security and privacy solutions in IoT(Fig.3). They discuss particularly the benefits that new approaches such as blockchain and Software Defined Networking can bring to the security and the privacy in IoT in terms of flexibility and scalability. Finally, they give a general classification of existing solutions and comparison based on important parameters.

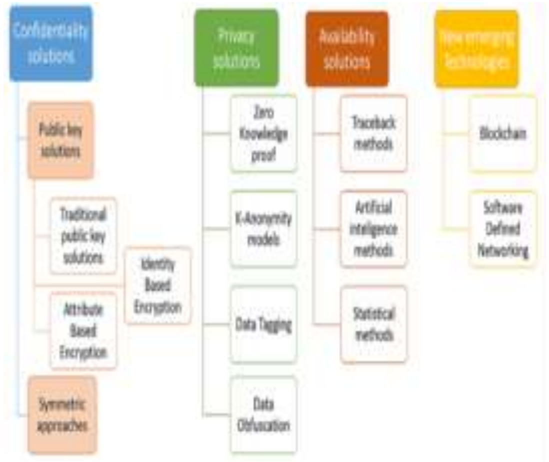

Fig.3. IoT Security Solutions

Hua Wang, Zonghua Zhang and Tarek Talebin in their research [13] show that, it is meaningful to develop IoT use cases, covering architecture, communication protocols, and applications and so on, and further conduct threat analysis for understanding the threat landscapes. As a matter of fact, it is said that many intelligent IoT devices nowadays are designed with ARM and Linux, which may contain a large number of vulnerable open source software especially the Linux kernels, thereby seriously threatening many IoT services and applications running with them.

C. Secure Integration

This paper [7] by Christos Stergiou et al, present a survey of IoT and Cloud Computing with a focus on the security issues of both technologies. Specifically, they combine the two technologies in order to examine the common features, and in order to discover the benefits of their integration. It shows how the Cloud Computing technology improves the function of the IoT. At the end, the security challenges of the integration of IoT and Cloud Computing were surveyed through the proposed algorithm model, and also there is a presentation of how the two encryption algorithms AES(Advanced Encryption Standard) and RSA(Ron Rivest, Adi Shamir, and Leonard Adleman), contributes in the integration of IoT and Cloud Computing.

A paper [14] by Alessio Botta et al, In this paper, focuses our attention on the integration of Cloud and IoT, which is what we call the CloudIoT paradigm. Many works in literature have surveyed Cloud and IoT separately and, more precisely, their main properties, features, underlying technologies, and open issues. However, to the best of our knowledge, these works lack a detailed analysis of the new CloudIoT paradigm, which involves completely new applications, challenges, and research issues. To bridge this gap, in this paper we provide a literature survey on the integration of Cloud and IoT. IoT is generally characterized by real world small things, widely distributed, with limited storage and processing capacity, which involve concerns regarding reliability, performance, security, and privacy.

D. Defense Mechanisms

S. Karthikeyan et al, in their study [4] suggest that even though there are mechanisms for the authentication of the devices or the humans, it is more reliable by making the authentication mechanism from X.509 digital certificates that have a significant impact on IoT security. These digital certificates have the ability to perform hashing, encryption and then signed digital certificate can be obtained that assures the security of the IoT devices. When IoT devices are integrated with X.509 authentication mechanism as shown in Fig.4, intruders or attackers will not be able to access the system that ensures the security of the devices. This study focuses on defense mechanism through X.509 digital certificates. This mechanism is present in between the communication devices and cloud storage.

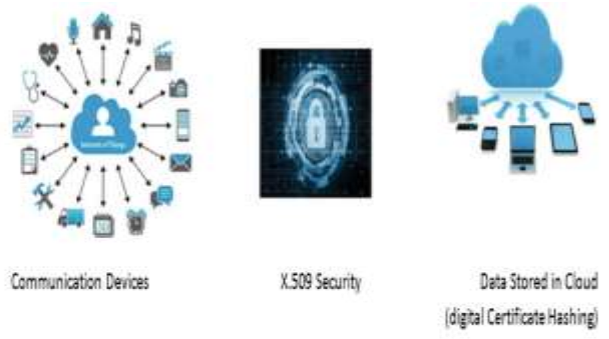

Fig.4. IoT Communication Security Using X.509

Tariq Ahamed Ahanger et al, [5] by their study have some of the common security breaches recognized to be relating to confidentiality of data, integrity of data, secure user authentication, and secure access control and such. As IoT applications can be accessed by multiple domains and has multiple user regimes, it requires security framework that enables users to have confidence in the data and services exchanged over the platform. In addition, new approaches use of machine learning/artificial intelligence in management of IoT, homomorphic encryption, searchable encryption and more are also promising security methods for this platform. Overall, their study also presented existing solutions exist for tackling these security issues.

Diego Rivera et al, have their paper [6], propose a series of security mechanisms to protect an IoT smart toy platform designed to help child development professionals in the early detection of psychomotor delays. These mechanisms have been determined by identifying the general and specific threats that could affect each part of the system and then providing solutions to mitigate or prevent them. It is proposed using standard security protocols and good practice techniques in each module, employing the technology available for Android tablets or computers for the application and collector/CDSS server, respectively. Furthermore, the connections between each sub module have been protected by standard protocols such as WPA2 and TLS when they use W-Fi and TCP/IP connections.

E. IoT Challenges

The paper [2] by Mohammad Wazida et al, discusses a generalized authentication model which can be used to perform authentication procedure among different communicating parties in order to secure remote surgery in the Tactile Internet (TI) environment. In their proposed authentication model, an authentication protocol can be designed so that an authenticated surgeon can use the robot/robotic arms to perform the surgery securely as well as remotely. To deal with this emerging research area, a secure mutual user authentication mechanism should be provided between a remote surgeon and the robot/robotic arms so that they can communicate securely using the established session key among them. Further, several security issues and challenges for such kind of communication are also discussed in this article.

Edewede Oriwoh et al, put forward a paper on IoT forensics [11] which has a scope being two-fold: firstly it proposes the application of a 1-2-3 Zones approach to Internet of Things (IoT)-related Digital Forensics (DF) investigations. Secondly, it introduces a Next-Best-Thing Triage (NBT) Model for use in conjunction with the 1-2-3 Zones approach where necessary and vice versa. These two ‘approaches’ are essential for the DF process from an IoT perspective: the atypical nature of IoT sources of evidence (i.e. Objects of Forensic Interest - OOFI), the pervasiveness of the IoT environment and its other unique attributes and the combination of these attributes dictate the necessity for a systematic DF approach to incidents.

Wei Zhou et al, in their research [16], first propose the concept of “IoT features”. Then, the security and privacy effects of eight IoT new features were discussed including the threats they cause, existing solutions and challenges yet to be solved. To help researchers follow the up-to-date works in this field. Their paper finally illustrates the developing trend of IoT security research and reveals how IoT features affect existing security research by investigating most existing research works related to IoT security from 2013 to 2017.

III. PROPOSED STATEMENT

The development of IoT security is an important part of IoT. As Data privacy and security continues to be the single largest issues in today’s interconnected world. Data is constantly being established, transmitted, stored and processed by large companies using a wide array of IoT devices, such as smart TVs, speakers and lighting systems, connected printers, HVAC systems, and smart thermostats.

The Internet of Things being a new technological advance, Ignorance of IoT security, both by companies and individual users, can increase the risks of cyber security caused due to lack of experience and the human factor.

And it’s just that IoT devices, regardless of their use or the range of information they collect from the user, are an attractive target for cybercriminals. We must not forget that the devices of the Internet of Things collect private information about the behavior of the user in certain areas such as finance, health, education and more, thereby increasing the threat level. The transmission of data by non-encrypted means presents a major security problem. Consider also the importance of network security, since the IoT is generally focused on mobile devices of various types and predominantly wireless networks.

A. Effective and Possible Solutions

1. Public Key Infrastructure:

The Public Key Infrastructure is “a set of policies, software/hardware, and procedures, which is required for the creation, management, and distribution of the digital certificates.” This security process has proven over the years to be an effective solution to IoT security issues.

PKI ensures the encryption of data through both asymmetric and symmetric encryption processes. In the former, both the data encryption and decryption is done with the same key while different keys are used for the data encryption and decryption in the latter. The data encryption and decryption ensure that data privacy is maintained and the chances of data theft are reduced to the bare minimum. Cryptographic key and X509 digital certificate are some IoT. PKI (Fig.5) security methods that can be used as well as public or private key management, distribution and revocation.

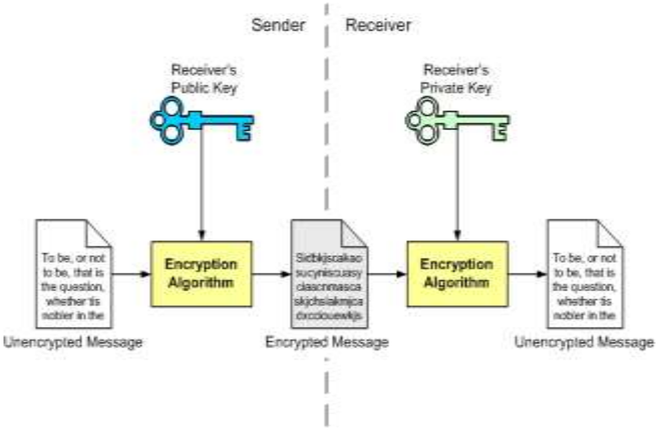
Sender
Receiver
Receiver's Public Key
Receiver's Private Key
To be, or not to be, that is the question, whether tis nobler in the
Encryption Algorithm
Sidbkjscakao sucyniscuasy claacnmasca skjchslakmjca dxcdouewkjs
Encryption Algorithm
To be, or not to be, that is the question, whether tis nobler in the
Unencrypted Message
Encrypted Message
Unencrypted Message

Fig.5. Public Key Infrastructure

2. Ensure Communication Protection:

The IoT concept works on communication between the connected devices. However, when communication is compromised, there will be a communication breakdown that can render the devices useless.

Many people do not know how to prevent putting themselves at risk online regularly. They don’t know that to ensure smooth communication always, the communication should be encrypted. The same principle applies to communication between the connected devices and the interface such as web apps and mobile apps.

Some notable encryptions that can be implemented are AES 256, HTTP, AES 128, and a host of others. This layer of protection renders the interface impregnable to potential hackers.

3. Secure the Network:

IoT devices are connected to back-end systems that are already connected to the Internet via an IoT network. This network plays a crucial role in the smooth operation of IoT devices. Some of the most required capabilities of a secure network are briefly discussed**.**

- Resilience to attacks: The system should be capable enough to recover itself in case if it crashes during data transmission. For an example, a server working in a multiuser environment, it must be intelligent and strong enough to protect itself from intruders or an eavesdropper.
- Data Authentication: The data and the associated information must be authenticated. An authentication mechanism is used to allow data transmission from only authentic devices.
- Access control: Only authorized persons are provided access control. The system administrator must control access to the users by managing their usernames and passwords and by defining their access rights so that different users can access only relevant portion of the database or programs.
- Client privacy: The data and information should be in safe hands. Personal data should only be accessed by authorized person to maintain the client privacy.

4. Ensure Device Authentication:

We can reduce our IoT devices’ vulnerability to attacks if we carry out a comprehensive device authentication for our devices. Thus by using theX.509 digital certificates, it can produce the device authentication with the accuracy of more than 84.7%. There are multiple authentication features that are available for IoT devices. Some, like digital certificates, two-factor authentication, and biometric, ensure that nobody can have unauthorized access to our devices. A potential attacker will need some personal information to gain access to the devices and pieces of information that you are the only one that has access to.

IV. CONCLUSION

In this survey we have presented the security issues present in each layer of IoT (Internet of Things) architecture, security and privacy of the data used by the devices connected through IoT, defense mechanisms to prevent any type of attack and along with the challenges faced by the IoT devices. Although using IoT devices is not a crime and poses zero threat, the vulnerability to attacks from the cyberspace makes it important that we secure our devices and reduce the exposure to attacks. It truly is a brave new world that promises many exciting opportunities. And it is a conversation we all need to start having now that we are to reap the benefits of the connected world.

REFERENCES

[1] “A Review of Current Security Issues in Internet of Things”, Mudassar Ahmad, Tanveer Younis, Muhammad AsifHabib, Rehan Ashraf, and Syed Hassan Ahmed

[2] “User Authentication in a Tactile Internet Based Remote Surgery Environment: Security Issues, Challenges, and Future Research Directions”, Mohammad Wazida , Ashok Kumar Dasb , Jong-Hyouk Lee

[3] “Internet of Things Security and Privacy”, Mehiar Dabbagh and Ammar Rayes

[4] “Enhancement of Security in the Internet of Things (IoT) by Using X.509 Authentication Mechanism”, S. Karthikeyan, Rizwan Patan and B. Balamurugan

[5] “Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms”, Tariq Ahamed Ahanger, Fellow IEEE, Abdullah Aljumah, Fellow IEEE

[6] “Secure Communications and Protected Data for a Internet of Things Smart Toy Platform”, Diego Rivera, Antonio Garc´ıa, Mar´ıa Luisa Mart´ın-Ru´ız, Bernardo Alarcos, Juan Ramon Velasco, Ana G ´omez Oliva

[7] “Secure integration of IoT and Cloud Computing”, Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim , Brij Gupta

[8] “Security Issues in the Internet of Things (IoT): A Comprehensive Study”, Mirza Abdur Razzaq, Sajid Habib Gill Khan, Muhammad Ali Qureshi SaleemUllah

[9] “Internet of Things and Security Issues”, Suchitra.C , Vandana C.P: IJCSMC, Vol. 5, Issue. 1, January 2016, pg.133 – 139

[10] “Survey on Security Issues of Internet of Things (IoT) Devices”, Ajish K S, AthiraPrem, Reshma R and Minu Lalitha Madhavu

[11] “Internet of Things Forensics: Challenges and Approaches”, Edewede Oriwoh, David Jazani, Gregory Epiphaniou and Paul Sant

[12] “Internet of things security: A top-down survey”, Djamel Eddine Kouicem, Abdelmadjid Bouabdallah, Hicham Lakhlef

[13] “Editorial: Special Issue on Security and Privacy of IoT”, Hua Wang, Zonghua Zhang, Tarek Taleb. Published online: 19 August 2017 # Springer Science+Business Media, LLC 2017

[14] “Integration of Cloud Computing and Internet of Things: a Survey”, Alessio Botta, Walter de Donato, Valerio Persico, Antonio Pescap´

[15] “A Review of Security Concerns in Internet of Things”, Engin Leloglu. Journal of Computer and Communications, 2017, 5, 121-136 http://www.scirp.org/journal/jcc ISSN Online: 2327-5227

[16] “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved”, Wei Zhou, Yuqing Zhang, and Peng Liu

[17] “A Survey on the Internet of Things Security”, Kai Zhao, LinaGe. 2013 Ninth International Conference on Computational Intelligence and Security