A Review on Security Concepts in IoT

Mr. Vinod Kumar[1], Dr. Sonia Vatta[2]

[1 2]Department of Computer Science & Engineering, Rayat Bahra University, Mohali

ABSTRACT – *Internet of Things is the intelligent connection of people, process, data and things. All communication in IoT is between machines (M2M) rather than people to people communication. This work presents a review on security concepts in IoT. It covers introduction, IoT overview and IoT security concepts. The research work of different researchers is presented here to find out the facts. This work will help in further developments in the field.*

Keywords: Internet of Things (IoT), challenges, encryption, security, protection.

***Corresponding Author**

Dr. Sonia Vatta
Department of Computer Science & Engineering, Rayat Bahra University, Mohali
sonia.vatta@rayatbahrauniversity.edu.in
Mr. Vinod Kumar
Department of Computer Science & Engineering, Rayat Bahra University, Mohali
786.vinod@gmail.com

1. INTRODUCTION

The concept of Internet of Things has gained significant traction over the last decade, owing to collective efforts by industry players, associations as well as academia. Various consortiums of corporate as well as industry associations have been working towards increasing worldwide IoT awareness and adoption [1].

The use Internet of Things (IoT) is increasing in the society, the NEW security challenge faced in IoT are becoming more critical day by day. Collection and shearing of data in the IoT is very important and plays significance role in the IoT. From a data communication perspective observations may provide a great help to understand IoT security [2].

This review study is focusing on two parts, one about the IoT security and other part on Growth and Challenges of IoT in India.

2. IoT OVERVIEW

In present days, the IoT is well known, subsequently the applications related to IoT are coming up and the industry will arise, for example CTS – cyber transportation systems, CPS – cyber physical systems and M@M- machine-to-machine communications.

For the security point of view, the IoT is facing challenges and will be faced with severe challenges. Following are the reasons: 1. The IoT is expending the 'internet', the traditional internet, sensor network, mobile network and so on, 2. Every 'thing' will be going to connected to the 'internet'. 3. The 'things' will be communicating with each other.

That will arise the new security and privacy problems. More attention is required to the issues for authenticity, confidentiality and integrity of data in the IOT [3]. The milieu intelligence and autonomous control are not the part of the concept of IoT. With the evolution of advanced network techniques, cloud computing and distributed control for multi-agent systems, that is a shift integration of the IoT concepts and self-governing control in M2M to produce an advancement of M2M in the form of CPS. CPS is focusing on interactive applications, real-time distributed control, cross layer and cross-domain optimization, intelligentization interaction etc. Therefore new technologies and methodologies are required to be developed to meet higher requirements of reliability, security and privacy [4].

3. IoT SECURITY CONCEPTS

The Internet of Things (IoT) is a marvel of technology development, which enhances more and more pervasive connectivity around the world. It expands the communication capability of in- formation and communication technologies (ICTs) from "Any TIME "and "Any PLACE" to "Any THING". However, on the other hand, it makes the security situation more and more severe.

Many of the researchers, from several different perspectives have published their surveys on security of IoT; some of them are summarized as below.

Wei Zhou, Yuqing Zhang, and Peng Liu, Member, IEEE(2018) gave ideas of "The New Features of IoT how Effect on Security and Privacy: Existing Solutions, New Threats and Challenges Yet to Be Solved".

The authors discussed about the new features of IoT and the security & privacy threads concerned, they also discussed about the existing solutions and challenges [5].

The author discussed about the IoT security:

- Find the basic issues of current IoT threats and challenges in IoT with the potential of "IoT features".
- Understand the effect of IoT characteristic, describes eight features which have most impact on security and privacy issues and threats, research challenges, and opportunities derived from each attribute.

- Trends of current IoT security, its development and cause based on IoT features, with the analysis of existing research in last five years.

The focus is on the eight features provided by IoT as Fig 1.

i. Interdependence
ii. Diversity
iii. Constrained
iv. Myriad
v. Unattended
vi. Intimacy
vii. Mobile
viii. Ubiquitous

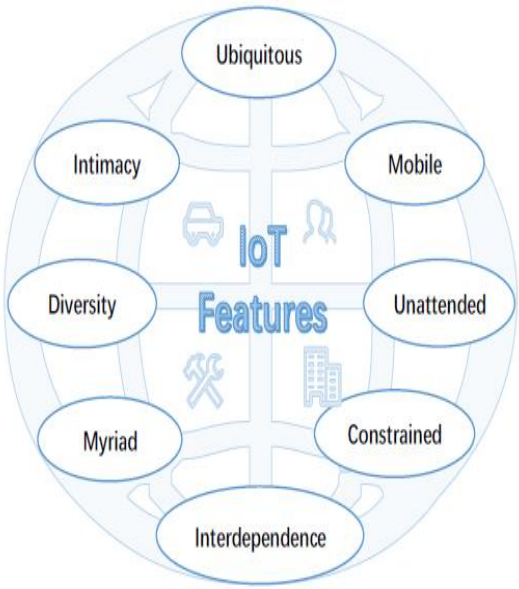

Fig. 1. IoT Features.

The summary of these eight features with Threat, Challenges and Opportunities is as TABLE 1:

TABLE I
THREATS, CHALLENGES, AND OPPORTUNITIES OF EACH IOT FEATURES

Feature	Threat	Challenge	Opportunity
Inter-dependence	Bypassing static defenses, Overprivilege	Access control and privilege management	Context-based permission
Diversity	Insecure protocols	Fragmented	Dynamic analysis simulation platform, IDS
Constrained	Insecure systems	Lightweight defenses and protocols	Combining biological and physical characteristics
Myriad	IoT botnet, DDoS	Intrusion detection and prevention	IDS
Unattended	Remote attack	Remote verification	Remote attestation, Lightweight trusted execution
Intimacy	Privacy leak	Privacy protection	Homomorphic encryption, Anonymous protocols
Mobile	Malware propagation	Cross-domain identification and trust	Dynamic configuration
Ubiquitous	Insecure configuration	\	Safety consciousness

The authors also discussed about the "IOT SECURITY RESEARCH ANALYSIS "Which discuss importance of research of security in IoT, The researchers should give attention to latest IoT applications, to overcome the possible threats before they appear.

Hui Suo, Jiafu Wan(2012) "Security in the Internet of Things: A Review"

The author explains the research status of key technologies like encryption mechanism, communication security, protecting sensor data and cryptographic algorithms and the challenges.

The security of information and network should be provisioned with the characteristics such as un-deniability, confidentiality, identification and integrity. Differentiating from internet, the IoT will be used to the crucial areas of national economy e.g. health care & medical service and, intelligent transportation. Therefore security needs in the IoT will be higher in-availability and dependency [6].

The security architecture in view of various layer like Application, support, network and perceptual layer as shown in Fig. 2 is identified by author.

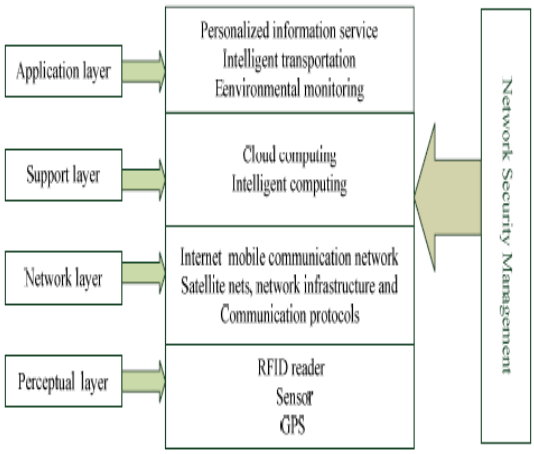

Figure 2. Security architecture

The perceptual layer (recognition layer) is most basic layer, It collects all type of information by physical equipments and identifies the physical world, the information contains environmental condition, object properties etc;

The next is network layer, Network layer is responsible for the authentic communication of information from perceptual layer, initial processing of information, polymerization and classification.

The next level is support layer. The support layer provides a definitive support platform to application layer, on support platform all type of intelligent computing powers will be managed through network grid and cloud computing.

The application layer is the uppermost level. Application layer deals with personalized services according to the users need.

Network security and the management is a very important factor in each level. The analysis of security requirements in each level is summarized as Figure 3.

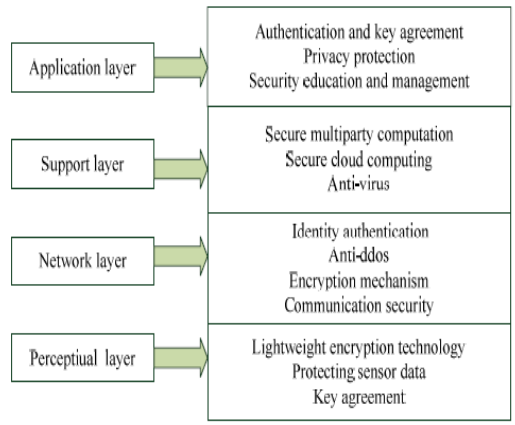

Figure 3. Security requirements in each level

Author discussed about "STATE OF CRUCIAL TECHNOLOGIES" like communication, security, encryption mechanism, protecting sensor data and cryptographic algorithms as below.

Encryption Mechanism

When the security requirement business is not very high, we can deal with by-hop encryption protection; when the needs are of high-security, then end-to-end encryption will be of first choice. According to the different requirements we select different encryption mechanism. Presently, IoT is in its primary stage and the safety mechanism is in the initial stages or not in the practice.

Communication Security

The botnets and DDoS attacks can harm the availability of communication media. When a larger-scale DDoS attacks occurs, how to deal is highly significant, more attention is required for preventive measures and disaster recovery methods.

Protecting Sensor Data

Guidelines are there to deal with protection of sensor data problem in design phase, first of all users must have information that they are being sensed, also users must have option to choose whether they are being sensed or not, and users must be capable of remaining anonymous.

Cryptographic Algorithms

Various algorithms like AES, RSA, DH, SHA-1 and SHA 256 are available; for the implementation of cryptographic algorithms resources are required such as memory, processor and speed. Till now it is not clear that how these cryptographic techniques can be applied in IoT, further research is required to ensure that algorithms can be successfully implemented using constrained of memory, speed and processor in the IoT.

FLAUZAC Olivier, GONZALEZ Carlos, NOLOT Florent (2015) "New Security Architecture for IoT Network"

The author explain Internet of Things (IoT) security architecture on the basis software-defined networking (SDN). The SDN-based architecture can work with or without infrastructure, that's we call SDN-Domain.

Recent research in computer networking introduced the paradigm for future communication, the Software Defined Networks (SDN). It is a central software program, called SDN controller, it manage the overall network behavior. The controller can add, update, and delete flow entries, in response to packets and proactively with predefined rules. In addition, SDN enables fast reaction to security threats, granular traffic filtering and dynamic security policies deployment [7].

The concept of grid of security network is to extend the SDN domain concept to multiple domains (Fig. 4) and each controller of each domain exchanges and security rules with controllers of the other domains. There are SDN controllers which behave as security barriers on the edge of the SDN Domain to ensure the network safety.

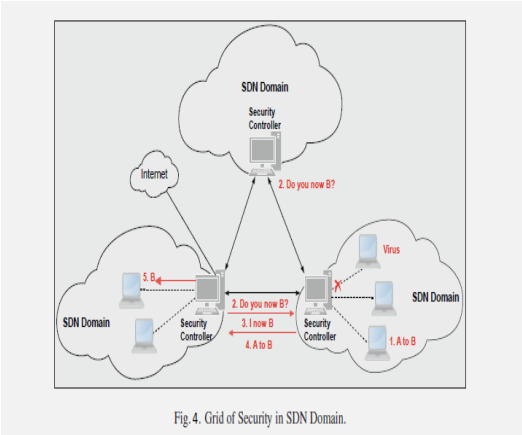

Fig. 4. Grid of Security in SDN Domain.

In every domain, there can be networks with or without infrastructure and for each domain the controller is responsible. There is a border controller that is responsible for communications between domains. In order to guarantee the independence of each domain in case of failure these edge Controllers have to work in a new distributed interaction. This architecture ensures the security of whole network with grid of security embedded in each controller to avoid attacks.

Sophia MOGANEDI (2017) "Beyond the Internet of Things convenience: Security and Privacy Concerns"

The author discusses the current security and privacy challenges presented by the increasing use of the IoT. He suggests possible solution to deal with these challenges. The proposed solution results can be implemented during the design, building, testing and deployment phases in the real-life environments of IoT to minimize the security and privacy challenges.

The work of authors suggests possible reasons for vulnerability and security weakness as follows:

a) IoT expands the concept of 'Internet' from traditional Internet to mobile networks and sensor networks.

b) IoT refers things connected to Internet.

c) These 'things' communicate with each other through internet.

IoT devices communication with each other and the data transmission becomes vulnerable and it is a challenge for network security. Because at network security level the on data during transmission can be exploit by several common types of attacks [8].

Which type of personal information needs to be protected becomes a matter of importance in order to preserve the personal privacy; particularly in wireless devices one can track the user's actions, location, behaviors, health status and preferences.

The author purpose IoT security Model (Figure 5).

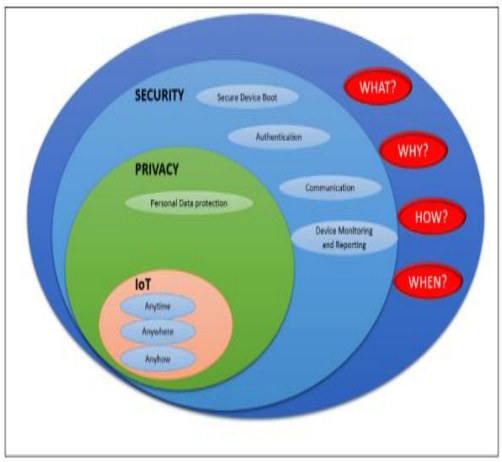

Figure 5 Proposed IoT Security Model

The aims of this model are to identify the following components in concern to employing security and privacy in the IoT domain:

- What –what needs to be secured and protected?
- Why – the reason for securing the IoT devices and preserving the personal privacy.
- How –mechanisms and methods that can be used to secure the IoT devices and preserve the personal privacy.
- When –the stages of security and privacy consideration and implementation.

The followings are addressed by the proposed Security Model:

- Device Boot
- Device Protection
- Communication
- Authentication
- Personal Data Protection
- Device Monitoring and Reporting
- Data Transmission Security

The security and privacy limitations represented in these solutions were taken into consideration. IoT Security Model address the limitations of the existing solutions with respect to security and privacy. This model can be used in the IoT application while designed, built, tested and deployed in the real-life environment to overcome the security and privacy challenges.

4. CONCLUSION

The IoT will change everyone's daily life. The short-range mobile will be the daily requirements. The environment of IoTs will change the way of communication, which will also increase the threat on privacy and data of users. The security implications of such an evolution should be carefully considered. The protection of data and privacy of users has been identified as one of the key challenges in the IoT. This work has presented various security issues at different layers in IoT. In addition, we identified several open issues related to the security which needs to be addressed by research community to make a secure and trusted platform for the delivery of future Internet of Things. It is concluded that by deeply analyzing new features of the Internet of Things, we can have a better plans for the future research of the IoT security.

REFERENCES

[1] Jaydip Sen, Internet of Things, Technology, Applications and Standardization, 2018.
[2] B,B Gupta, Megha Quamara, Internet of Things Security, 2020.
[3] Sridipta Misra, Salman Hashmi, Security Challenges and Approaches in Internet of Things, 2017.
[4] Pardeep Kumar, IoT Security: Advances in Authentication, 2020.
[5] Wei Zhou, Yuqing Zhang, and Peng Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE, 2018.
[6] Hui Suo, Jiafu Wan, "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering, 2012.
[7] FLAUZAC Olivier, GONZALEZ Carlos, NOLOT Florent , "New Security Architecture for IoT Network", Science Direct, Procedia Computer Science 52, 1028 – 1033, 2015.
[8] Sophia MOGANEDI, "Beyond the Convenience of the Internet of Things: Security and Privacy Concerns". Research Gate Conference Paper, DOI: 10.23919/ISTAFRICA.2017.8102372, 2017.