International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 05, 2020
ISSN: 1475-7192

Security Threats and Mitigation Approaches in IoT based Applications

Dr.A.P. Nirmala

Abstract--- *The Internet of Things (IoT) as a budding technology has modernized the global network comprising of people, smart devices, intelligent objects, information, and data. There is a huge opportunity for IoT to make the world more available, integral, accessible, confidential, interoperable and scalable. IoT can be exercised In domains such as, healthcare, transportation, entertainment, power grids and smart buildings. IoT is likely to work as a catalyst for the future technological innovations and its use is presumed to grow rapidly. Various devices which we use on a daily basis can connect with each other via internet; this has been made possible by IoT. There remain security concerns due to the connection of numerous devices to the internet and the massive data associated with it. Protection and integration of heterogeneous smart devices and information communication technologies (ICT) are the significant factors of the paradigm. The security threats that the users face in the environment of IoT and countermeasures to mitigate them, are discussed in this paper.*

Keywords--- *Internet of Things, Protocols, Architecture, Security Threats, Healthcare, Home Appliances, Smart Phones.*

I. INTRODUCTION

IoT is a system of things which has progressed from mobiles and computers linked over internet in the past years to the new era with the advent of new technologies, things like security cameras, microwaves, cars and industrial equipment's are connected to internet. Some applications (e. g., smart electric meter reading, greenhouse monitoring, telemedicine monitoring, and intelligent transportation) have made the conception of IoT has mainly been accepted in the recent years [12]. It is observed that the number of connected devices around the world will dramatically increase from 20.35 billion in 2017 to 75.44 billion in 2025. International Data Corporation (IDC) has predicted at 17.0% compound annual growth rate (CAGR) in IoT spending from $698.6 billion in 2015 to nearly $1.3 trillion in 2019 [16].

Thus, provides opportunity for hackers to use these devices will enlarge to their advantage through ‘denial of service’ attacks, malicious e-mail, and other harmful worms and Trojans. According to several studies, 70% of IoT devices are susceptible to attacks. A recent test conducted by HP discovered that 90 percent of the tested devices collected at least one piece of personal information via the product itself, the cloud or its mobile application. Cyber attack or unauthorized access can easily negotiate this personal information, this will lead to uncertainty for the users to adopt this technology due to reduction in confidentiality, integrity and security of the data [10].

The paper is organized as follows: Section II provides an analysis on security challenges in the field of IoT

Dr.A.P. Nirmala , Associate Professor, Dept. of MCA, New Horizon College of Engineering, Bengaluru, India.
E-mail: nirmlasuresh.ap@gmail.com

DOI: 10.37200/IJPR/V24I5/PR2020694
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

which are adiscussed in few related works. Section III discusses an overview of protocols and architecture for IoT along with the key layers that make up IoT. Section IV describes the security threats in IoT based domains and countermeasures to mitigate the security threats. Section V gives conclusion and future directions.

II. RELATED WORK

As a budding field, IoT has some open concerns especially on the security issues such as Identifying and locating object, authentication and authorization, privacy, Lightweight Cryptosystems and security protocols, software vulnerability and operating system platforms [8].

The spectrum of research necessary to attain IoT at the scale visualized above needs a lot of research in many directions. Problems and required research in 8 topic namely massive scaling, architecture and dependencies, creating knowledge and big data, robustness, openness, security, privacy, and human-in the-loop are focused by John A. Stankovic et al. [11]. New problems that arise for future IoT systems are primarily concentrated in each of the topic discussions.

IoT Security Problem and results to the problem or measures to avoid them were put forward by Annamalai et al. [3] and Yang Lu et al. [4]. They conferred on IoT cyber security architecture and taxonomy, key enabling countermeasures and approaches, major applications in industries, research trends and confrontations.

Some of the critical issues related to the wide use of IoT are security and privacy. These concerns do not allow wide adaptability of IoT. Therefore, the authors in these paper [9][10], presented a general idea about the various layered architectures of IoT and damages regarding security in each layers. An analysis that provides solutions to these issues is presented with their confines. In addition, a new secure layered architecture of IoT was suggested to outlook these issues.

According to S. Naik et al. [1], IoT's Top Security Concerns are: Device Cloning, Sensitive Data Exposure, Denial of Service, Unauthorized Device Access and Control, Tampering Data. Their study explained the need to alleviate IoT security confrontations, Device Cloning and Sensitive Data Exposure. W. Zhou et al.[16] described eight features which have most impact on security and privacy issues and discuss the threats, research challenges, and opportunities derived from Inter- dependence, Diversity, Myriad, Unattended, Intimacy, Mobile and Ubiquitous. The security challenges such as Unauthorized Interference between communicating parties, Eavesdropping attack, Trust management, NVMs (non-volatile memories) susceptible to physical attacks, Data Confidentiality, Data Integrity & Data

Availability, Device-to-Device identification (Information Privacy), Access Control, Insurance of security and privacy needs in heterogeneous environment were stated [17].

III. PROTOCOLS AND ARCHITECTURE IN IOT

IoT interlinks the globe and cyberspace through physical objects that implant into intelligent sensors and thus resulting in a trade of data by more than 20 million Internet- Connected objects. Standard interaction protocols are necessary in building interlinked and interoperable smart objects. International organizations

DOI: 10.37200/IJPR/V24I5/PR2020694
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

such as the Internet Engineering Task Force (IETF) and the IPSO Alliance, promote the use of Internet Protocol (IP) as the standard means for interoperability of smart objects. IPv6 is found likely to be a solution for smart-object interaction since billions of objects are expected to be connected and IPv4 addresses have almost reached exhaustion. The protocol stack that smart-objects will implement will try to match classical Internet hosts in order to make it practical to create the so-called Extended Internet, that is, the aggregation of the Internet with the IoT. Since the protocol structural design of smart objects should remain the standard IP architecture, many of the security mechanisms presently used for the Internet can be reused in IoT set-ups [10].

In order to achieve the object of creating secured and reliable IoT, the following four layers play a vital role which is shown in the architecture of IoT in Fig. 1.

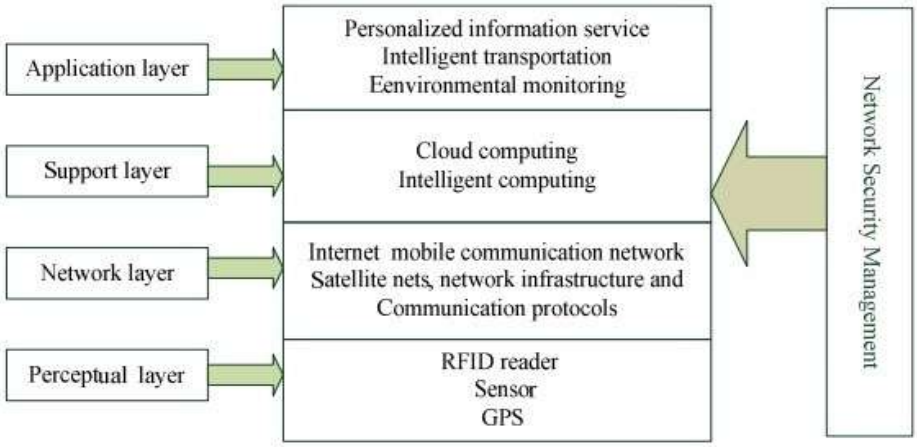

Fig. 1: Security Architecture

- Application Layer: This layer includes applications and services that the IoT offers. Some of the applications can be seen in smart cities, smart home, transportation, utilities and healthcare [15]
- Perception Layer: Sensory technologies of various forms, including temperature sensors, vibration sensors, pressure sensors, and RFID sensors that allow devices to sense other objects are present in this layer [14]
- Network Layer: This layer consists of network communications software as well as physical components such as topologies, servers, network nodes, and network components that allow the devices to communicate. Its main purpose is to transmit data between devices and from the devices to receivers [13]
- Physical Layer: Basic hardware such as physical components, smart appliances and power supplies that acts as backbone for networking the smart objects is included in the physical layer.

IV. Security Threats in IoT and Counter Measures

A large number of software security solutions are present in PCs and mobiles to guard them from most of the damages but such security solutions are absent in the rest of the IoT. To launch a DDoS attack, thousands of security cameras were breached; which caused a twitter outage. An entire ecosystem of hardware, software,

DOI: 10.37200/IJPR/V24I5/PR2020694
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

cloud, web and mobile interface is an IoT solution. Since this network is not very mature, there are still major concerns lurking around IoT implementation is largely due to security threats [1], protecting IoT is a difficult task.

The IoT will face more severe confrontations as to the security. The reasons are as follows:

1) the 'internet' is unmitigated by the IoT via traditional internet, mobile and network sensors, and so on. 2) The 'internet' will be the hub every 'thing' will be connected to it. 3) These 'things' will correspond with each other. This will lead to rise in confidentiality problems. The research issues for confidentiality, authenticity, integrity of data in the IoT should be given attention. The original perception at this stage does not include the ambient intelligence and autonomous control. Development of complex network techniques, dispersed multi-agent control and cloud computing, leads to a shift in incorporating the concepts of IoT and autonomous control in Machine to Machine (M2M) research to bring a progression of M2M in the form of CPS (Cyber Physical Systems). The main focus of CPS is on intelligentization of interaction, interactive applications, distributed real-time control, cross-layer and cross-domain optimization, etc. In order to meet the higher necessities in terms of reliability, security and privacy, some new technologies and methodologies should be developed [12].

Privacy basically means that the data of the user is in his or her control and no one else can approach it. Reliability is another problem that evolves with a very high reliance on the data and devices based on IoT. Working efficiently as expected at all times without breakdown is what we mean by reliability of the devices. Data transmission between devices and the Internet should be reliable in addition to IoT, since giving incorrect information or giving unreliable data is a grave trepidation as this might lead to taking unnecessary consequences [10]

The properties such as identification, confidentially, integrity and non-deniability should help in providing the security of information and network. Vital areas of economy will need the application of IoT, e.g., medical service and health care, and intelligent transportation, thus security needs in the IoT will be higher in availability and dependability [12].

A primary crisis that is persistent in the Internet now-a- days that must be solved is dealing with security attacks. Security attacks are troublesome for the IoT since the smallest possible capability of "things" (devices) being utilized, the physical convenience to sensors, actuators and objects, and the directness of the systems, including the fact that most devices are linked wirelessly.

IoT applications must be able to continue to operate satisfactorily in the presence of, and to recover effectively from security attacks. This section focuses on the security threats in various applications and discusses the ways to mitigate it.

A. Security Threats in IoT based Domains

1. *Smart manufacturing:* The fourth industrial revolution (Industry 4.0) has emerged from IoT and provides a great advantage by connecting people, processes and data. Cyber- attacks from criminals,

DOI: 10.37200/IJPR/V24I5/PR2020694
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

terrorists and hackers which pressurizes cyber security and has become a major challenge to IoT enabled CPS. Cyber security is vital for the achievement of smart manufacturing. Advancement in computation along with other computational ability will play a crucial role for cyber security, such as development of artificial immune system for IoT security architecture, data mining/fusion in IoT allowed cyber physical systems, and data driven cyber security [5].

2. *Home Appliances:* The advancement of smart devices to home automation is to allow devices to interlink over the Internet. Though linking household appliances to the Internet has been made more easily and effective, the risks posed by interlinking these appliances has increased since vulnerabilities exist that have a possibility to be overcome [6].
3. *Smart Phones:* Smartphone is one of IoT's chief constituent; therefore it should be more secure and private. Infringement of security can be categorized as Breach of confidentiality, Breach of Integrity, Breach of availability, Denial of service and theft of service. A broad description of the various security issues in smart phones which are the fundamental parts of IoT are provided by M. H. Khan et al. [7].
4. *Information Security:* As IoT growth is enormous, the issues in providing security on information which are shared among various objects and devices [2].
5. *Healthcare:* In a situation where an interfering signal to block an infinite communication line between an RFID tag and a reader in IoT, or even spoof an RFID tag to send an error note to the user by invaders can lead to confusion in the medical information system and can affect the security of patients [4]. The above example explains how wireless wearable devices can utilize IoT-derived data to enhance basic operations. This initiates the need for security and privacy in use of IoT in healthcare.

B. Counter Measures to Mitigate the Security Threats

According to M. H. Khan et al. [7], multifaceted and minor networks and systems should be protected and identified quickly from malware and attacking terminals.

1. *Smart Refrigerator:* Digital crimes like identity theft, spamming, privacy, data loss and so forth through creation of IoT bot can be identified and transmitted by an instrument called the "smart refrigerator". Smart Refrigerator Crime Propagation (SRCP) Model [6] showed how vulnerabilities are able to be overcome. In addition, the authors also found the necessary countermeasures which have digital forensic means to filter periodic contact to and from the refrigerator in a forensic to approach specific data in an IoT-based environment.
2. *Digital watermarks:* Multimedia data, such as digital images, audio and video sequences are safe guarded by Digital watermarks. It is unique and generally invisible marks that are present in digital objects, include information about the possessor of these objects, they are also used in detecting falsifications.
3. *Self-healing:* Self healing is defending action towards an attack. A system needs to sense the attack, diagnose it, and set up countermeasures and maintenances, and most importantly carry out all the processes in a lightweight approach due to the various low capacity devices concerned. In the present

DOI: 10.37200/IJPR/V24I5/PR2020694
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

era, security solutions need heavyweight computations and huge memory requirements, so solutions for IoT are the main research confrontations [11].

In some cases, healing requires re-programming, for e.g., when an unforeseen attack takes place. In that case, healing commands need to be securely (with authentication and verification) delivered to the appropriate nodes and then the node's managing programs need to be modified by the runtime structural design. Unique hardware support will be needed to encrypt, authenticate, verify, and tamper proof keys. Production with heritage devices will be established complex, on development of security-aware devices.

A specific approach is implicated that merges the utilization of unique technologies in the design of IoT system which includes: exercising digital watermarks in joining cryptographic means of protecting information in the broadcasted messages, utilizing typical filters and protocols to transfer the data, employing network monitoring systems and automatic information processing tools while the produced messages are being found. This tactic is used to resolve the issues while automatic processing of massive circulated messages are forwarded to IoT systems [3].

V. CONCLUSION

IoT is a developing area of the Internet and it is rising rapidly along with applications of Internet in the present day and age. IoT allows easy interaction between machines and objects. IoT facilitates the intelligence to affix several essential features of modernization, such as homes, hospitals, buildings, transports and cities. A general idea of protocols and structural design of IoT, confrontations in IoT security and precautions against such challenges are presented in this paper. This paper also provides information on IoT security challenges and promotes people to do further researches and make future choices for studying in this field.

REFERENCES

[1] S. Naik and V. Maral, Cyber security — IoT, 2017 *2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, pp. 764-767, 2017.

[2] B. Usmonov, A. Iskhakov, A. Shelupanov, A. Iskhakova, and R. Meshcheryakov, The cybersecurity in development of IoT embedded technologies, *Int. Conf. Inf. Sci. Commun. Technol.*, pp. 1–4, 2017

[3] Annamalai, Lakshmanan and Selvakumar Manickam, A Literature review on Cyber Security in the field of IoT–Internet of Things, Technical Report, April, 2018.

[4] Yang Lu; Li Da Xu, Internet of Things (IoT) Cybersecurity Research: *A Review of Current Research Topics, IEEE Internet of Things Journal*, September 2018

[5] H. He C. Maple T. Watson A. Tiwari J. Mehnen Y. Jin B. Gabrys, The Security Challenges in the IoT enabled Cyber-Physical Systems and Opportunities for Evolutionary Computing & Other Computational Intelligence, Evolutionary Computation pp. 1015- 1021 2016

[6] Kebande, Victor R., Nickson M. Karie, Antonia Michael, Semaka MG Malapane, and H. S. Venter, How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime, *IST-Africa Week Conference (IST-Africa)*, pp. 1-10. IEEE, 2017.

[7] M.H. Khan M.A. Shah, Survey on Srecurity Threats of Smartphones in Internet of Things, Automation and Computing (ICAC) 22nd International Conference, 2016.

[8] Gupta, Krishna Kanth, and Sapna Shukla. Internet of Things: Security challenges for next generation networks. *International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, pp. 315-318. IEEE, 2016.

[9] Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.-S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors 18*, 2796. 2018,

DOI: 10.37200/IJPR/V24I5/PR2020694
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

[10] Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava, Security in Internet of Things: Challenges, Solutions and Future Directions, IEEE 49th *Hawaii International Conference on System Sciences (HICSS)*, pp. 5772-5781, 2016

[11] John A. Stankovic, Research Directions for the Internet of Things, *IEEE Internet of Things Journal*, Vol. 1, Feb. 2014.

[12] Hi Suo, Jiafu, Caifeng Zoua, Jianqi Liua Wan. Security in the Internet of Things – A Review, International Conference on Computer Science and Electronics Engineering (ICCSEE), pp. 648 –651, 2012

[13] Xu Xiaohui. Study on Security Problems and Key Technologies of The Internet of Things, Fifth *International Conference on Computational and Information Sciences (ICCIS)*, pp.407–410, 2013

[14] Sathish J Kumar and Dhiren R Patel. Article: A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications* 90(11):20-26, March 2014.

[15] K. Fazal, H. Shehzad, A. Tasneem, A. Dawood, Z. Ahmed, A Systematic Literature Review on the Security Challenges of Internet of Things and their Classification, *IJTNR*, PP.40-48, 2017

[16] W. Zhou, Y. Jia, A. Peng, Y. Zhang, P. Liu, The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved, *IEEE Internet Things J.* 12, 1–1, 2018.

[17] I. Yaqoob, E. Ahmed, I.A.T. Hashem, A.I.A. Ahmed, A. Gani, M. Imran, and M. Guizani, Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges, *IEEE Wireless Communications*, vol. 24, no. 3, pp. 10–16, June 2017.

DOI: 10.37200/IJPR/V24I5/PR2020694
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020