2019 4th International Electrical Engineering Conference (IEEC 2019)
Jan, 2019 at IEP Centre, Karachi, Pakistan

Security, Privacy, and Trust in IoT

Faizan Hussain[1], Syed Daniyal Nadeem[1], Aqeel-ur-Rehman[1], and Sadiq ur Rehman[2]

[1]Department of Computing, Hamdard Institute of Engineering and Technology, Hamdard University
[2]Department of Electrical Engineering, Hamdard Institute of Engineering and Technology, Hamdard University
Karachi, 74600, Pakistan

Abstract: Internet of things is reaching new peaks and rapidly gaining momentum and popularity in many domains of our daily lives. These domains include vehicles, industry, education, agriculture, hospitals, environmental monitoring etc. In every aspect, internet of things (IoT) has its marks and milestones which are gradually increasing as the technology is getting advanced and handy to use. Internet of things (IoT) brings the multitude of technologies and techniques together with the vision of creating the organized and interconnected world so the communication between entities can be done in a better, usable and efficient manner. Security, privacy, authentication, and trustworthiness for the end users is considered to be the main feature for any technology. An important and essential role is played by security, trust, and privacy for the satisfaction of end users. Most commonly observed requirements for IoT security are namely authentication, confidentiality and access control. There are several available ways in which security, privacy, and trust of IoT can be managed in which NFC, RFID, and WSN are commonly used.

Keywords: Trust. WSN, Security, IoT, Privacy

I. INTRODUCTION

There are several available definitions of an Internet of things which is commonly written in short abbreviation as "IoT". IoT is embedded with several sensors, actuators, different software's with the connectivity of the internet to gather, exchange, and collect the data further[1], it forms an effective and vital global network structure with many self-configuring abilities, it characterizes and represents the interconnection of several "things", sensors, and smart devices. Fig. 1 shows the applications, areas, and usage of IoT in our daily routines and lives.

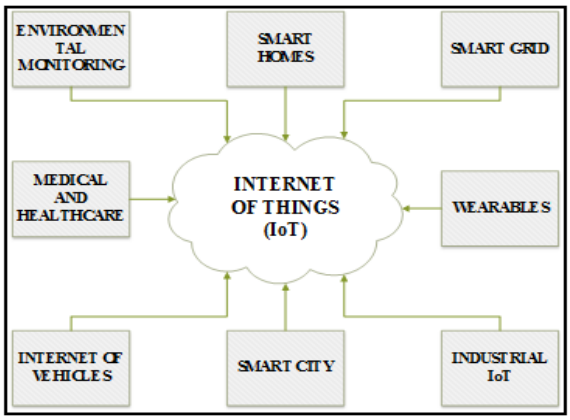

Fig. 1 Internet of Things and Applications

There are several scenarios in which IoT application are commonly used which includes mobility, transportation, smart homes, smart engineering or manufacturing methods, smart energy grids and networks [2].

IoT provides the services in a more effective and efficient way. However, there are some critical factors that come along with the advancement of technology, some of these factors are namely security, privacy, and trust of the end user. There are some limitations which may bound IoT in some spaces. There are some well know projects in the field of IoT which focused on the security aspect and their comparison can be seen in table 1.

Table 1. Projects focusing on IoT security

Projects	Authentication	Confidentiality	Trust	Privacy
Butler [3]	✓	✓	×	✓
EBBITS [4]	×	✓	×	×
Hydra [5]	×	✓	×	×
uTRUSTit [6]	✓	×	✓	×
iCore [7]	✓	✓	✓	✓
HACMS	✓	✓	×	×
NSF [8]	✓	✓	✓	✓

This paper is divided into IX sections, Section I is the introduction, the difference between traditional internet and IoT is presented in section II. Security, privacy and trust in the IoT is covered in section III. Section IV coves IoT security requirements. Security, privacy and trust in IoT, IoT protocols related to security and issues and challenges are presented in section V, VI, VII respectively. Section VIII is about the open challenges and finally, the conclusion can be seen in section IX.

II. TRADITIONAL INTERNET AND INTERNET OF THINGS

The transformation between traditional internet and internet of things (IoT) is the absence of human role [1]. The services, facilities provided by the applications or

devices used in the internet of things (IoT) offers an effective and efficient benefit to human lives. The words "Internet" and "Things" is considered to be a single word now which gives an impression of connecting different physical devices of different standards from all around the word on to the internet for the purpose of exchanging information [9].

Area	Traditional Internet	Internet of Things (IoT)
Content	Human creates content	Machine creates content
Content Consumed	By generating request	By triggering actions and pushing information
Content Combined	Using links (explicitly)	Using operators (explicitly)
Data	Generate with the help of peoples	Generate with the help of sensors (e.g. Temperature, pressure)
Efficient	Increase and covers internet efficiency	Add intelligence to the procedure

Table 2. Difference between Traditional Internet and IoT

III. SECURITY, PRIVACY, AND TRUST IN THE INTERNET OF THINGS

Security plays an important role in terms of usability, efficiency, and reliability in IoT.

The need for privacy is the core property of self-actualization in IoT. There are several applications working in many different grounds like patient monitoring system, traffic control, energy consumption inventory management, smart parking, civil protection any many others. Privacy should be guaranteed to the end user.

After security, the main aspect occurs is the privacy and with privacy, there is trust (see Fig. 2), according to the internet of things, trust is also an important aspect or factor which is developed by the end user when there is an element of security and privacy in the device.

Some of the key issues and challenges regarding security, privacy, and trust can be seen in section VII.

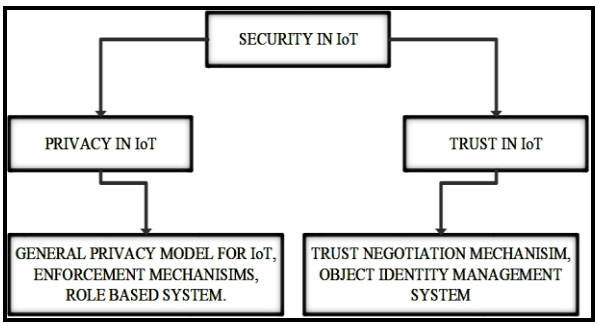

Fig. 2 Dependency of Privacy and Trust on Security

IV. IoT SECURITY REQUIREMENTS

The three basic requirements for the internet of thing's security [10][11] are namely authentication/integrity, confidentiality, and access control. IoT enables to share, configure, transfer the data from the end user to the other destination of different standard, version, protocols etc. To achieve the goal, security plays a major role from one end to another.

A. Authentication

IoT devices must establish authentication, non-repudiation, integrity at several levels. Which is used to help devices to communication between the users and built the trust among each other [12].

B. Confidentiality

Confidentiality is important for IoT in a way that the wireless communication between one object to other different objects is particularly sensitive and vulnerable to confidentiality threats. Attackers are always snooping for confidential data and information for their use. Message or data may easily get intercepted by the adversaries for the transmitting medium.

C. Access Control

It discusses the permission in the usage of resources and data assigned to different devices of the wide and vast area of the IoT networks. Data holder and data collector are present when dealing with access control in IoT. All the information need to be placed according to the instruction given by data holders. Data collector must collect the specific and targeted data so that the process of authentication and identification of genuine data holder can be performed.

V. WAYS FOR SECURITY, PRIVACY, AND TRUST IN IoT

Some of the IoT core technologies include radio frequency identification (RFID), near field communication (NFC), wireless sensor networks (WSN) [13]. Automated information in the internet of things exchanges between 2 devices or 2 ends takes place through some communication technologies which are described below [14].

A. NFC

Near field communication (NFC) is a type of contactless communication which is considered to be the important technology for IoT. As the name says, this technology is only usable when devices need to exchange their data within a short distance. NFC is

commonly used in smart cards, transportation, healthcare, access control etc. [15].

B. WSN

Wireless sensor networks (WSNs) play important functions in the internet of things. Wireless sensors networks are the arrangements of independent nodes whose wireless interaction and communication takes place over restricted or having limitation in the place and bandwidth. A typical WSN consists of microcontroller, sensor, memory, transceiver and a power supply or battery [16]. Wireless sensor networks contain many advantages due to its features of intelligence and efficient processing [13]. WSN perform the computation by three fundamental components hardware, software, and algorithm respectively.

C. RFID

According to [17] [18], radio frequency identification (RFID) is one of the essential factors in the IoT and its applications. It is a major innovation in embedded transmission and communication criterion or paradigm which allows the design of microchips for wireless communications. RFID helps to do the identification by using a unique id or a barcode in an automated way. The detailed concept of RFID is discussed in [18].

VI. IoT PROTOCOLS RELATED TO SECURITY

IoT covers a large range of applications, products, and technologies. For this reason, numbers of protocols related to the security for IoT are getting increased. A comparison on some of the most important protocols working at different layers in IoT can be seen in Table 3. A detailed concept about these protocols used in IoT is discussed in [19] [20].

Table 3. The stack of protocol related security.

Layer	Protocol	Security Protocol	Inter-operability	Manage-ability	Security
Application	CoAP, MQTT	User-defined	Yes	Yes	Yes
Transport	UDP	DTLS	Yes	Yes	Yes
Network	IPv6, RPL	IPsec, RPL security	Yes	-	Yes
6LoWPAN	6LoWPAN	None	-	Yes	Yes
Data-Link	IEEE 802.15.4	802.15.4 security	Yes	-	-

VII. ISSUES AND CHALLENGES

In this section, issues regarding security, privacy, and trust in IoT will be discussed in detail.

A. Issues regarding security in the Internet of things

Security issues in IoT can be divided into four major sections which are as follows:

1. Identification

It is important to maintain and manage the identity in devices and application. Identification can be either M2M or H2M. In both ways, it should be manageable and maintain in order to keep all the security aspects.

2. Authentication

Authentication is one of the major issues in IoT to make synchronization and maintain data authentication especially when the area is big.

3. Data Management

Data is a major factor for IoT. As with the advancement of device and applications, data from different standards of objects are in use. There are several techniques that can be utilized for identification of the objects in the internet of things. Some of them are Vision-based object identification, Barcode recognition, and identification etc.

4. Heterogeneity

Internet of things is that kind of emerging technology which allows all sort of objects and devices to connect with each other which bring issues regarding the security. Table 4 presents the solutions regarding issues discussed above.

Table 4. Area of Issues and their Solutions

Area of Issues	Solutions
Authentication	Handshaking of algorithms and pre-shared keys for low power availability. RFID plays the main part in the recognition and identification of entities.
Identification	Considering their physical address and by the use of IPv6
Data management	Databases software (e.g. SQL, SQL lite etc.)
Heterogeneity	Architecture known as IDRA must be used which is particularly intended to participate in all the devices. IDRA can attach objects directly without any gateway. It covers backward compatibility and requests fewer properties.

B. Privacy issues in the Internet of things

Many devices are connected together, working together in both public and in private domain. There is a tinny or small difference among security and privacy, mostly security avoid to exchange and process personal information. Security constraints are mainly confidentiality, authentication, and integrity but privacy typically define as verifiability, transparency, and right purpose [21]. Privacy is important to identify the authorized end user, user privacy, access control, to do

secure communications, resilience to attacks, and the most important to build the trust level between the device or application and the end user.

C. Trust issues in the Internet of things

Trust is developed when there are security and privacy in the object or entity. Trust is a very multifaceted concept that is influenced by many measurable and non-measurable belongings or parameters. It is associated to security and user safety in different facets of the entity, trust covers a big area as compare to security and privacy thus it is not as much as easy to build and accomplished the trust factor. Another important concept connected to trust is privacy that is the capability of an object to control whether, when, and to whom information about itself is to be released or disclosed a detailed discussion is in the paper [22].

VIII. OPEN CHALLENGES

IoT is an advance and new era's topic. The concept of IoT is an immense topic connecting billions of things together with full efficiency and usability. To manage such big data, heterogeneous networking environments, and secure information and communication technologies, is really a big research challenge [21]. Some of the areas are listed below which will also represent the open challenges and issues.

- How to achieve complete interoperability
- To design efficient, less energy and fast encryption algorithm
- Unique identification method for each device/application
- To decentralized the authentication and trust
- The symmetric key management scheme
- Privacy framework for heterogeneous systems
- Standardization
- Security and Privacy Protection
- Development strategies

IX. CONCLUSION

As we have discussed in this paper about the security, privacy, and trust that what is security, trust, privacy, importance, needs, issues, and challenges. IoT is an emerging technology rapidly gaining importance from last decade we have to know about the major and basic concepts of internet of things in order to perform and use the technology in our daily routines, IoT is not only used in a specific zone but it is used and applied on multiple zones either it is homes, grid, health care, industry, agriculture, and other entities because of that we have to know about the IoT and the important aspects of it, the concept of IoT is to play safe and secure by ensuring about the privacy from which the trust built and the technology can get more useable and advance in the future as the needs increases once the trust, privacy and security factor builds.

REFERENCES

[1] Sgora, D. D. Vergados, and P. Chatzimisios, "A survey on security and privacy issues in Wireless Mesh Networks," Secure. Commun. Networks, vol. 9, no. 13, pp. 1877–1889, 2016.

[2] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," Proc. - 2015 Int. Work. Secure. Internet Things, SIoT 2015, pp. 49–57, 2016.

[3] Macagnano, Davide, Giuseppe Destino, and Giuseppe Abreu. "Indoor positioning: A key enabling technology for IoT applications." In Internet of Things (WF-IoT), 2014 IEEE World Forum on, pp. 117-118. IEEE, 2014.

[4] Vlacheas, Panagiotis, Raffaele Giaffreda, Vera Stavroulaki, Dimitris Kelaidonis, Vassilis Foteinos, George Poulios, Panagiotis Demestichas, Andrey Somov, Abdur Rahim Biswas, and Klaus Moessner. "Enabling smart cities through a cognitive management framework for the internet of things." IEEE communications magazine 51, no. 6 (2013): 102-111.

[5] Ngu, Anne H., Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z. Sheng. "IoT middleware: A survey on issues and enabling technologies." IEEE Internet of Things Journal 4, no. 1 (2017): 1-20.

[6] Hochleitner, Christina, Cornelia Graf, Peter Wolkerstorfer, and Manfred Tscheligi. "uTRUSTit–Usable Trust in the Internet of Things." In International Conference on Trust, Privacy and Security in Digital Business, pp. 220-221. Springer, Berlin, Heidelberg, 2012.

[7] Nambi, SN Akshay Uttama, Chayan Sarkar, R. Venkatesha Prasad, and Abdur Rahim. "A unified semantic knowledge base for IoT." In Internet of Things (WF-IoT), 2014 IEEE World Forum on, pp. 575-580. IEEE, 2014.

[8] Gazis, Vangelis, Manuel Goertz, Marco Huber, Alessandro Leonardi, Kostas Mathioudakis, Alexander Wiesmaier, and Florian Zeiger. "Short paper: IoT: Challenges, projects, architectures." In Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on, pp. 145-147. IEEE, 2015.

[9] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015.

[10] W. Trappe, R. Howard, and R. S. Moore, “Low-energy security: Limits and opportunities in the internet of things,” IEEE Secur. Priv., vol. 13, no. 1, pp. 14–21, 2015.

[11] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in the Internet of things: The road ahead,” Comput. Networks, vol. 76, no. March 2017, pp. 146–164, 2015.

[12] Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, “Anonymous authentication for privacy-preserving IoT target-driven applications,” Comput. Secur., vol. 37, pp. 111–123, 2013.

[13] Rehman, S. Rehman, I. U. Khan, M. Moiz, and S. Hasan, “Security and Privacy Issues in IoT,” Int. J. Commun. Networks Inf. Secur., vol. 8, no. 3, pp. 147–158, 2016.

[14] T. Borgohain, U. Kumar, and S. Sanyal, “Survey of Security and Privacy Issues of Internet of Things,” arXiv Prepr. arXiv1501.02211, p. 7, 2015.

[15] P. Urien, “LLCPS: A new security framework based on

TLS for NFC P2P applications in the Internet of Things," 2013 IEEE 10th Consum. Commun. Netw. Conf. CCNC 2013, pp. 845–846, 2013.

[16] D. Systems and S. Modes, "1. Introduction," no. i, pp. 1–15, 2009.

[17] E. Welbourne et al., "Building the Internet of Things Using RFID," Internet Comput. IEEE, vol. 13, no. 3, pp. 48–55, 2009.

[18] Juels, "RSA Laboratories - RFID Security and Privacy: A Research Survey," J. Sel. Areas Commun., vol. 24, no. 2, pp. 381–394, 2006.

[19] S. Deshmukh and S. S. Sonavane, "Security protocols for Internet of Things: A survey," 2017 Int. Conf. Nextgen Electron. Technol. Silicon to Software, ICNETS2 2017, pp. 71–74, 2017.

[20] "IoT Standards & Protocols Guide | 2018 Comparisons on Network, Wireless Comms, Security, Industrial", Postscapes, 2018. [Online]. Available: https://www.postscapes.com/internet-of-things-protocols/.

[21] K. Laeeq and J. Shamsi, "A Study of Security Issues, Vulnerabilities, and Challenges in the Internet of Things," Secur. Cyber-Physical Syst., pp. 221–240, 2015.

[22] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120–134, 2014.