Global Journal on Application of Data Science and Internet of Things
Vol. 2, Issue 2 - 2018

STUDY OF PRIVACY ISSUES IN INTERNET OF THINGS

MAMTA YADAV[*], JYOTIR MOY CHATTERJEE[**]

ABSTRACT

The Internet of Things (IoT) prototype gives a general view on interdependence of smart things over the current and future Internet framework is an emanating field which evolves all over the world and it correlates the common object with the connected devices. It gives an emerging platform with greater flexibility to the people, so that they can interact with the surrounding things. It is not only providing the facility to consumer domain but also for the industrial field. IoT pervasiveness increases by utilizing the various growing applications such as radio-frequency identification (RFID), and wireless sensor networks (WSNs). To understand the emerging technologies of IoT in industry, this research work reviews the works of researcher on major IOT application areas in industries and identifies the various privacy issues of it.

KEYWORDS: Internet Of Things (Iot), Radio-Frequency Identification (RFID), And Wireless Sensor Networks (Wsns.)

INTRODUCTION

IoT is an emerging technology which provides ubiquitous collaboration of devices or objects at any moment and at any place [1]. In1999, Kevin Ashton at Procter & Gamble was first used the term “IoT” for describing the Internet based service architecture gives a concept for connecting and coordinating the billions or even trillions of Internet enabled devices to accomplish a specific target [2]. IoT plays a major role on many different industrial areas such as transportation, health care and manufacturing industries and provides a promising solution for them. Earlier, IoT refers to connect the internet enabled objects with radio-frequency identification (RFID) technology then afterwards IoT is also correlates with many technologies like sensors, GPS devices and mobile devices etc. It provides a platform to connect the various surrounding devices with the Internet and also describes how to integrate the different technologies such as sensors, actuators, GPS devices and mobile devices with it [3]. IoT refers to utilize many different smart devices for sensing, transferring and evaluating/ processing the collected data from surrounding environment and then gives the result back to the environment. IoT makes the people’s life easier and effortless. Now a day, IoT technology is used in many various industries areas like agriculture, food processing industry, environmental monitoring, security surveillance and etc. Many research works have been implemented on industrial IoT.

[*]M.Tech (CT-CSE), RCET Bhilai (CG), LBEF (APUTI), Kathmandu, Nepal.
[**]Assistant Professor (IT), LBEF (APUTI), Kathmandu, Nepal.
Correspondence E-mail Id: editor@eurekajournals.com

ISSN: 2581-4370

For example, a device computes the heart beat rate and body temperature and this data is forwarded to energy management system to regulate the room temperature by depending upon the person's physiological status. The acquired data can be shared with many different contributors or service providers for improving the business intelligence. Meanwhile, we assume that the sharing and providing the authority to access the private collected data or information with the different stakeholders or third parties should be protected [2]. Those devices which are connected through IoT generates, evaluates, process and transfer the private data or information, thus it may be affected through various cyber-attacks. It is very critical in IoT system to guarantee that the integrity of data will be maintained with the embedded devices after destructive or harmful attacks. Many research work and studies have done on security of data with the underlying devices [4].

IoT defines an infrastructure where the physical devices and sensors associated with these devices are connected through wireless or wired internet. Different types of LANs are available for connection with sensors like RFID, NFC, Wi-fi, Bluetooth and many more [5]. IoT consists of two terms- 'Internet' and 'Things'. The first term 'Internet' relates the IoT with network oriented, while the term 'Things' related with the integration of objects which are existing in physical world into a common framework. However, the combination of these two terms reveals that IoT provides a system of interrelated objects which are uniquely identifiable in globally and based on the various interoperable communication protocols [6].

IoT is implemented by using the general layered architecture shows in Figure 1. This architecture is developed for various different industries, organization, institutes, governments and etc. There are 5 layers defined below [6]:

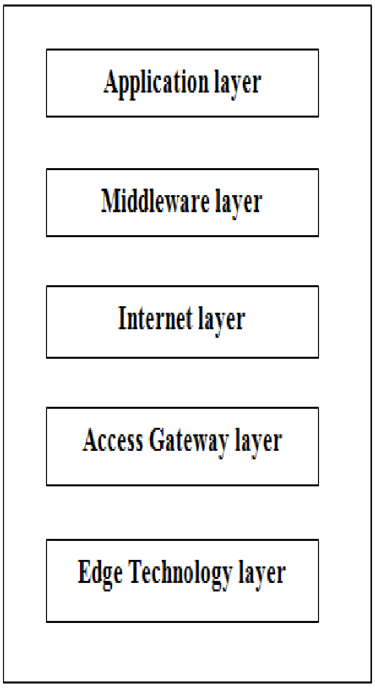

Figure 1.Generic Layered Architecture of IoT

a. **EDGE TECHNOLOGY LAYER:** Consists of sensors, actuators embedded systems, RFID tags and etc. These elements identify and store information (RFID tags), collects information (sensor), process (embedded system), communicate and control.

b. **ACCESS GATEWAY LAYER:** Data handling is performed at this layer. It keeps track of message routing, producing and arrangement of message data.

c. **INTERNET LAYER:** It provides the interface between Access Gateway and Middleware layer. Function of this layer is to transfer the data through wireless or wired connections.

d. **MIDDLEWARE LAYER:** This layer acts in bi-directional way and operates as an interface between Edge technology layer and Application layer. This layer provides device management, information management, access control, information discovery, semantic analysis and data filtering and aggregation.

e. **APPLICATION LAYER:** This is the topmost layer and provides the functions to the various users of IoT which are involved in many different industries such as manufacturing, retailing, health care, public safety, home support, security, surveillance, food and drug and many more.

INDUSTRIAL APPLICATIONS OF IOT

a. **IoT IN HEALTHCARE INDUSTRY**: By using the various features of IoT such as recognition, sense and communication in healthcare industry for tracking and surveillance of people, medicines and diagnostic equipment. IoT provides the new opportunities for enhancing the development of this industry. All the information (such as administration, diagnosis, therapy, finance and etc.) related to this field can be gathered, manage and shared effectively and efficiently through IoT [3].

b. **IoT IN FIREFIGHTING FIELD:** With the help of IoT, possible fire catastrophe has been detected by giving the proper early warning signal. In China, researchers used RFID tags and/or bar codes for making the automatic alarming system for development of the country. Security and privacy of the data are the two main challenges in this field by leveraging the IoT systems [3].

c. **IoT IN TRANSPORTATION AND LOGISTICS:** IoT has been used to track and monitor the movement of physical devices from source to destination through supply chain path i.e. manufacturing, transporting, distributing and etc. By utilizing the IoT embedded features such as RFID tags, sensors, WLNs developed a system for monitoring the atmospheric moisture of the system [7].Here also, maintaining security and privacy of the information are the challenging task through IoT.

d. **IoT IN MINING INDUSTRY:** IoT technologies plays an important role in this field. IoT has been used to detect the disaster in underground mines and to give the proper warning signals for safety improvement. Many IoT technologies such as RFID tags, WLNs, WiFi and etc. devices are used to monitor the exact position of underground miners for improving the security and privacy measures [3].

e. **IoT IN AUTOMOBILE INDUSTRY:** The evolution of automotive industry existed very earlier but the new revolution has been available now just because of IoT technologies in such a way that the vehicles or cars driven by humans previously are now through fast developing technology is driven by themselves or driverless. Several WLNs, WiFi, Bluetooth and cellular communication technologies of IoT are used for developing the fully automated cars [8].

f. **IoT IN AGRICULTURE INDUSTRY:** Agriculture plays a crucial role for the development of the nation. Many research works have been done to make the modernizing system i.e. from traditional system to smart agriculture system by leveraging the IoT technologies. Control operations performed through interfacing devices such as sensors, WiFi, actuators and etc. As IoT is associated with many devices which may cause to possible entries of malwares and it may create security risks [9].

RELATED WORK

2009 [14] analyzes the problems faced by people in today's life of IoT in the context of privacy. Researcher gives the concept of secure multi-party computation for preservation of privacy in the different ubiquitous field of IoT. The main disadvantage of SMC protocol is its ineffective and it can affect its applicability.

2010 [25] presented & reported on the architecture of the Privacy Coach, and shown how it enables users to make informed privacy decisions in a user-friendly manner.

2011 [6] illustrated the state of the art of IoT and its technological drivers. Researchers highlight the various applications of IoT and its challenges also. And at last, identified and described the issues of IoT which can across in near future.

2012 [26] presented SHARDIS, a P2P-based discovery service architecture for the EPC global Network that enhances client privacy by applying secret-sharing on the information documents of interest.

2013 [27] present a fully decentralized anonymous authentication protocol aimed at encouraging the implementation of privacy-preserving IoT target-driven applications.

2014 [3] reviewed the recently research work on IoT in different industries. Firstly, describes the SOA models of IoT and the technologies associated with it. After that, they highlighted some industrial applications of IoT and its challenges. And also gives the possible opportunities of it.

2014 [13] discussed about the privacy and security issues of Internet of things. As IoT systems provides services for improvement in people's life style or make their life easier. If IoT is not implemented in correct manner then it can harm the people's life also through privacy threats. Here the challenge is to design a promising solution which makes proper balance between the requirements of business interests and customer's privacy. The researchers of this paper analyze the privacy threats of IoT and its challenges in four steps. The first step highlights the privacy threats of IoT and triggers the need of detailed analysis for it. Secondly, discussed about the evolution of IoT which not only focuses the general view but also privacy threats view. In third step, summarizes the privacy threats into seven types. Lastly, discussed about the technical challenges associated with each threat and also gives clear vision for near future.

2015 [4] provides an overview about Industrial IoT and its related security and privacy challenges, and also gives the comprehensive security framework for Industrial IoT. Now a days; every object or devices are embedded with electronics and which in turn used for computation, identification, communication and many more. The interconnected network of smart object or devices universally is known as IoT and which is used in various industrial applications. But in today's life style, IoT system is not able to provide fully functional security and privacy threats. In this research paper, a comprehensive cyber security framework as solution for the above problem is provided in the industrial field.

2015 [1] aim to give the overview of IoT in terms of security and privacy. In this paper, researchers define the security architecture of IoT and also highlighted the security threats and privacy issues involved in each layer of architecture. At last researchers illustrates the need of more research work has to be done towards the security and privacy issues of IoT.

2016 [9] aims to provide the opportunities and challenges in agriculture industry of IoT based. As in our country, 70% depends on agriculture and the issues associated with it act as a barrier in the development of the nation. Hence, the researchers aim to makes the agriculture system smart through IoT technologies. Several embedded devices are used such as sensors, WiFi, camera, actuators with micro controller and raspberry pi.

2017 [12] presented two different systems for Industrial IoT based on wood industry. The aim of this approach is to maximize the profit in the market. The first prototype manages the data i.e. collecting, storing, analyzing and processing. The past as well as future estimated data or information can be collected through forecast procedure for it. The second prototype system is a simple and low cost. This system uses sensors and a Sensor Hub system which gathers, transmit, store and process the sensor data. This system analyzes the collected data and helps in decision making approach.

2017 [15] illustrates the various security threats involved in the automation field. Researchers of this paper summarize the security issues in the architecture of IoT at different layers. They also highlight the various mitigation practices required in the security layered architecture of IoT to solve the problem related to physical equipment, communication and data processing field. They found that the vulnerabilities of WSNs nodes used in IoT cannot be solved directly, some more research work has to been done on it.

2018 [10] provides the solution for Industrial IoT. This paper gives a general view for Industrial IoT by defining its architecture and standards. Researchers highlighted the concept of IoT, Industrial IoT and Industry 4.0. They discussed about the opportunities and challenges faced in Industrial IoT. They give the direction and solution for Industrial IoT through state-of-the-art research efforts.

2018 [11] proposed a security-by-design method for Industrial IoT. This method provides analyses the security and reduces the threats associated with it. There are two types of level defined in it i.e. design/modeling and runtime/simulation. The aim of this method is to analyze the security requirements and also to identify the paths which are affected and mitigate them. Researchers performed this task through a case study on maritime sector in a critical environment.

2018[29] provided insight to the dynamics that come with the emergence of IoT in the furniture & kitchen manufacturing industry.

2018[30] tried to provide insights about the advancements on IoT with IoC from a class review of published articles from 2009 to 2017.

2018[31] tried to provide better understanding between the IoT & BD, the insights of IoT on BD, the BD propels & the issues.

2019 [28] proposes a privacy preserving solution in ITS context relying on a game theory model between two actors (data holder and data requester) using an incentive motivation against a privacy concession or leading an active attack.

COMPARATIVE ANALYSIS

Sl. No.	Year of Publication	Advantages	Limitations
	2019 [17]	In this paper, proposed a game theoretical model as a solution for preserving the privacy of IoT in Intelligent Transportation Systems between data holder (driver) and requester (supplier). Theyillu strateeach transition state of player by using Markovian chain and also evaluated the	Aim to develop a new approach for determining the behavior and type of new player. And also require more attention on the long-termplayer’s reward and their effects during the game.

		utility function for making the balance between privacy concession and incentive motivation.	
	2018 [19]	Researcher provides a privacy preserving Social Internet of Things (SIoT) framework for profile matching of human centric networks. Firstly, researchers make the profile of their user to which they are associated with IoT devices and finally they provide the profile matching crypto-primitive framework named fuzzy vault based on Block Chain concept as a trust model.	This research work requires a more trusted Block Chain model for providing the more security.
	2018 [16]	This paper presented the design and implementation of a privacy framework of IoT.The researchers proposed the Advanced Encryption Standard (AES) architecture and its integration of framework in detail.	For solving the security problems, more advanced cryptographic techniques must be applied such as Public key Cryptography, Hashing, Digital signature and Cryptography Pseudo Random number generator.
	2018 [16]	This paper furnishes WSN (Wireless Sensor Network) architecture for monitoring the automation technologies and for highlighting its limitations. Also describes that how this architecture is useful in industries by giving the knowledge about techniques, protocols and its standards.	Advanced techniques and technologies are required for improvement in the WSN architecture.
	2018 [21]	Proposed Efficient and Privacy-preserving trafficobfuscation (EPIC) framework from traffic analysis attacks on smart homes. This framework provides privacy preserving mechanism and also to minimize the network utility cost.	As the proposed approach is unable to defend the attacks because of its various limitations, so there is a need to connect the wireless network with the devices for providing the smart's home privacy.
	2018 [22]	Researchers of this paper, proposed a new communication efficient privacy preserving range query method based on Fog-enhanced IoT. With the help of this method, query range and IoT device data are preserved by BGN homomorphic encryption technique. Additionally, this method also applies range query expression, decomposition and composition	Aims to develop a multi-range privacy preserving query function based on fog-enhanced IoT.

		technique to attain O ($\sqrt{n}$) communication efficiency.	
	2017 [18]	Researcher of this paper provides an authentication service between smart phone and smart home IoT devices by using QR codes and attributes-based cryptography. And also proposed a model for privacy preservation authentication between the IoT devices and cloud computing by applying the combination of two techniques such as FIDO and U-Prove.	In near future, researcher will aim to provide privacy preservation scheme for smart city by using FIDO and U-Prove technologies. And also intended to give authentication and authorization model for privacy preservation.
	2017 [23]	Proposed a Lightweight Privacy-preserving Data Aggregation (LPDA) method for fog-computing- enhanced IoT. This method aims to combine hybrid IoT devices and to also early injected false data at the network level by utilizing homomorphic Paillier encryption, Chinese Remainder Theorem, and one-way hash chain techniques.	In near future, researcher need to focus on some new real life IoT framework.
	2017[24]	Researchers of this paper proposed a modular Arithmetic Algorithm (MAPP) for privacy preservation in IoT. The aim of this method is to develop an algorithm to preserve the data against any type of threats by using CupCarbon 3.0 for simulation.	Aims to simulate and apply at very large scale and requires a comparison with another related algorithm.
	2016 [8]	The aim of this paper is to give more stress on industrial issues and challenges of full autonomous vehicles/cars through IoT technology.	Through the potential of this approach, the fully automated car can be seen by 2020 with the help of DSRC (Dedicated Short-range Communications) and 5G technologies.
	2016[20]	paper aims to utilize the combinational approach of cloud computing and IoT in health care domain for providing the privacy preservation to the end users and service providers. Researcher proposed cloud-based health care model for preserving the privacy using Organization for Economic Cooperation and Development (OECD) principle.	Improving the performance in near future requires more promoting techniques and protocols for ensuring the privacy.

DISCUSSION

Today, Internet of Things (IoT) is one of the most emerging technologies that open the way for the development of the Industries. But with the emergence of IoT, it is not able to satisfy the required functional as well as privacy and security need [4]. As IoT provides a ubiquitous infrastructure by connecting the common devices or objects with the network. The main reason of accepting IoT in several industries by manufacturer, developers and healthcare providers for development of the production system and also to achieve efficient result [10]. With the rapid growth of IoT technologies in industries, security and privacy are the two major concerns associated with it.In the upcoming years, more advance research is required in various industrial areas for the implementation of IoT in context of reliability, robustness and efficiency[6].This paper presented an overview of IoT with the help of layered architecture, the different application areas of IoT in the field of industries and the security and privacy issues of it. The main aim is to review the different research work done of the researchers who implemented the IoT technologies in industries and also analyze the various challenges came into existence.

REFERENCES

[1]. Vikas, B. O. (2015). Internet of things (iot): A survey on privacy issues and security. International Journal of Scientific Research in Science, Engineering and Technology, 1(3), 168-173.

[2]. Aleisa, N., & Renaud, K. (2016). Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion). arXiv preprint arXiv:1611.03340.

[3]. Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10(4), 2233-2243.

[4]. Sadeghi, A. R., Wachsmann, C., &Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE (pp. 1-6). IEEE.

[5]. https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf

[6]. Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49-69.

[7]. Zhang, Y., Chen, B., & Lu, X. (2011, August). Intelligent monitoring system on refrigerator trucks based on the internet of things. In International Conference on Wireless Communications and Applications (pp. 201-206). Springer, Berlin, Heidelberg.

[8]. Krasniqi, X., &Hajrizi, E. (2016). Use of IoT technology to drive the automotive industry from connected to full autonomous vehicles. IFAC-PapersOnLine, 49(29), 269-274.

[9]. Mehta, A., & Patel, S. (2016). IOT based smart agriculture research opportunities and challenges. Int. J. Technol. Res. Eng, 4, 541-543.

[10]. Sisinni, E., Saifullah, A., Han, S., Jennehag, U., &Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics, 14(11), 4724-4734.

[11]. Mouratidis, H., &Diamantopoulou, V. (2018). A Security Analysis Method for Industrial Internet of Things. IEEE Transactions on Industrial Informatics.

[12]. Pödör, Z., Gludovátz, A., Bacsárdi, L., Erdei, I., & Janky, F. N. (2017). Industrial IoT techniques and solutions in wood industrial manufactures. Info communications Journal, 9(4), 24-30.

[13]. Ziegeldorf, J. H., Morchon, O. G., &Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. Security and

Communication Networks, 7(12), 2728-2742.

[14]. Oleshchuk, V. (2009, May). Internet of things and privacy preserving technologies. In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on (pp. 336-340). IEEE.

[15]. Varga, P., Plosz, S., Soos, G., &Hegedus, C. (2017, May). Security threats and issues in automation IoT. In Factory Communication Systems (WFCS), 2017 IEEE 13th International Workshop on (pp. 1-6). IEEE.

[16]. Panagiotou, P., Sklavos, N., &Zaharakis, I. D. (2018, August). Design and Implementation of a Privacy Framework for the Internet of Things (IoT). In 2018 21st Euromicro Conference on Digital System Design (DSD) (pp. 586-591). IEEE.Raposo, D., Rodrigues, A., Sinche, S., Sá Silva, J., &Boavida, F. (2018). Industrial IOT monitoring: Technologies and architecture proposal. Sensors, 18(10), 3568.

[17]. Sfar, A. R., Challal, Y., Moyal, P., &Natalizio, E. (2019). A Game Theoretic Approach for Privacy Preserving Model in IoT-Based Transportation. IEEE Transactions on Intelligent Transportation Systems.

[18]. Togan, M., Chifor, B. C., Florea, I., & Gugulea, G. (2017, June). A smart-phone based privacy-preserving security framework for IoT devices. In Electronics, Computers and Artificial Intelligence (ECAI), 2017 9th International Conference on (pp. 1-7). IEEE.

[19]. Zouari, J., Hamdi, M., &Kom, T. H. (2018, June). Privacy Preserving Profile Matching Protocol for Human-Centric Social Internet of Things. In 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) (pp. 181-186). IEEE.

[20]. Elmisery, A. M., Rho, S., & Botvich, D. (2016). A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things. IEEE Access, 4, 8418-8441.

[21]. Liu, J., Zhang, C., & Fang, Y. (2018). EPIC: A Differential Privacy Framework to Defend Smart Homes against Internet Traffic Analysis. IEEE Internet of Things Journal, 5(2), 1206-1217.

[22]. Lu, R. (2018). A New Communication-Efficient Privacy-Preserving Range Query Scheme in Fog-Enhanced IoT. IEEE Internet of Things Journal.

[23]. Lu, R., Heung, K., Lashkari, A. H., &Ghorbani, A. A. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. IEEE Access, 5, 3302-3312.

[24]. Gheisari, M., Wang, G., Bhuiyan, M. Z. A., & Zhang, W. (2017, December). MAPP: A Modular Arithmetic Algorithm for Privacy Preserving in IoT. In Ubiquitous Computing and Communications (ISPA/IUCC), 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on (pp. 897-903). IEEE.

[25]. Broenink, G., Hoepman, J. H., Hof, C. V. T., Van Kranenburg, R., Smits, D., & Wisman, T. (2010). The privacy coach: Supporting customer privacy in the internet of things. arXiv preprint arXiv:1001.4459.

[26]. Fabian, B., Ermakova, T., & Muller, C. (2012). SHARDIS: A privacy-enhanced discovery service for RFID-based product information. IEEE Transactions on Industrial Informatics, 8(3), 707-718.

[27]. Alcaide, A., Palomar, E., Montero-Castillo, J., & Ribagorda, A. (2013). Anonymous authentication for privacy-preserving IoT target-driven applications. Computers & Security, 37, 111-123.

[28]. Sfar, A. R., Challal, Y., Moyal, P., & Natalizio, E. (2019). A Game Theoretic

Approach for Privacy Preserving Model in IoT-Based Transportation. IEEE Transactions on Intelligent Transportation Systems.

[29]. Chatterjee, J. M., Kumar, R., Khari, M., Hung, D. T., & Le, D. N. (2018). Internet of Things based system for Smart Kitchen. International Journal of Engineering and Manufacturing, 8(4), 29.

[30]. Jha, S., Kumar, R., Chatterjee, J. M., & Khari, M. (2018). Collaborative hand shaking approaches between internet of computing and internet of things towards a smart world: a review from 2009-2017. Telecommunication Systems, 1-18.

[31]. Chatterjee, J. (2018). IoT with Big Data Framework using Machine Learning Approach. International Journal of Machine Learning and Networked Collaborative Engineering, 2(02), 75-85.