User Privacy in IOT

Jawwad Ibrahim, Maria Iltaf, Naeem Saleem, Kamran Younas, Attiq Ahmed Khan

Abstract—Internet of things (IOT) is growing and relatively new technology using wireless Sensor Networks (WSN) and IP based communication. Participation of large number of devices and there mobility make it more and more challenging in term of connectivity, security and user privacy. In this paper we are going to analyze the technological aspect regarding network technologies, security and user privacy issues and suggest measures for improvements of user privacy in such ubiquitous networks. Because of unattended nature of IOT devices regular connectivity and security related issues always will be there and these are of our major concerns to make the network more secure. This paper is going to focus specially user privacy in this wireless nature of the networks, where user is not fully aware with the data collection and its usage. Normally, data is collected more than required, it must be according to actual needs and its usage should be accordance with collection purpose to maintain the user privacy. By maintaining most of the storage and control of information processing at provider's place not at cloud or other third party setups and furthermore private and public key combination encryption during data communication will enhance the privacy of user in such type of environments.

Index Terms— Internet of Things (IOT), Wireless Sensor Networks (WSN), Connectivity, Security, User Privacy, IOT Clouds.

1 Introduction

The internet of things, also called Internet of objects, refers to a wireless network between objects usually the network will be wireless and self-configuring, such as household appliances. The IOT will change everything including ourselves. The Internet of Things can be measured as new wave in Internet development. Internet of Things has ability to connect devices can range from smart house hold appliance to Self - Flying Pilotless planes and hi tech Drones. In simple words, IOT can be defined as "any-time, any-place and any-one connected technology which is based on technology which make things and people get closer to each other."

IOT is an emerging technology which has been involved in nearly every field of life. Concept of smart homes, smart buildings and smart cities is now present in reality and making differences in human's lives. IOT in many important and critical fields like healthcare management, supply chain management and in enterprise processes playing vital role to facilitate from the individual to enterprise level. As IOT is going to make influence in all business areas in future, the rest of paper is organized as follows. In section I we will discuss the literature review of IOT. In section II technological specifications and layers in IOT. In section III Threats to IOT specially user privacy and finally in section IV Measures need to be taken to improve the user privacy in IOT.

- *Jawwad Ibrahim*, *Lecturer in University of Lahore. Pakistan, E-mail: jawad.ibrahim@cs.uol.edu.pk*
- *Maria Latif*, *Lecturer in University of Lahore, Pakistan. E-mail: maria.latif@cs.uol.edu.pk*
- *Naeem Saleem is currently pursuing masters degree program in Computer Science in University of Lahore, Pakistan. E-mail: pugc06@gmail.com*
- *Kamran Younas is currently pursuing masters degree program in Computer Science in University of Lahore, Pakistan. E-mail: mrjarral11@gmail.com*
- *Attiq Ahmed Khan is currently pursuing masters degree program in Computer Science in University of Lahore, Pakistan. E-mail: attiqahmedkhan@gmail.com*

2 Literature Review

The rise of IoT has promising effects on people's lives in many areas including transportation, healthcare, commerce and household equipment. IoT devices collect data from real world and transmit it to cloud servers to process and store. Data gathered by remote devices can contain sensitive side channel information that may goes beyond the purpose for which the data collected. This area of user privacy and data security need to be focus and make user private up to certain possible limit in such ubiquitous environment. By using differential privacy we can deal with this threat of user privacy. Differential privacy is a class of techniques that add probabilistic transformations to each data item in a large database to prevent any individual from being identified from the larger set. [1, 3]

Key challenges in Internet of Things are data security and user privacy. IoT systems are highly at risk due to dynamic, mobile and physically unprotected nature. For better security and privacy encryption protocols to be efficient and scalable, software protection techniques should be improved for small devices. Existing encryption techniques like RSA and DES need to be revisit for small devices where it costly due to its computational capabilities. [2]

IoT has been widely applied in many fields of life, requiring huge volume of data to be processed; devices don't have the capacity and always resorts to the cloud for outsourced storage and computation, which has brought series of security and privacy threats. We can reduce these kinds of threats without exploiting pubic key homomorphism encryption; furthermore exploit it to address secure packet forwarding by aggregated transmission evidence to resist layer attacks and by applying privacy preserving message filtering in cloud IoT [3 , 12].

IoT have various benefits for humans as devices include sensors which enhance the security and can monitor the health of people. But these devices are usually energy efficient. Because of energy efficiency they tend to suppress the complex encryption standards which cause to render energy. But this affects the privacy and it becomes easy to collect the user information. [4]

In this IoTs era, the short-range mobile devices are implanted in our daily requirements. The communication between people and between object to object is gradually increased. Objects can locate each other in any time. The efficiency of information communication and management has risen to a new height. The security and privacy implications of such evolution should be carefully considered to new technology. The protection of data and privacy of users has been identified as one of the key challenges in the IoT [5].

Due to rapid growth of internet and communication technology, we are now led to an imaginary space of virtual world. IoT is relatively new area of technology and its certain limitations led to security and privacy concerns. Privacy breach threat is present at different levels, for example at device level, at processing level, during communication and at storage level. There are several open issues related to the security and privacy that need to be addressed by research community to make secure and trusted platform in the future. Lot of knotty problems are waiting for researcher to deal with [6].

Mobile and embedded systems are found everywhere and its application are also in manufacturing industry where it is a source of interactive manufacturing and modern processing branch of industry, it also produce and process huge amount of sensitive and private data. This privacy needs to be source from attackers and hackers targeting such private and sensitive data. This needs holistic security approach and resist the design of present industrial internet of things to make it secure and trust worthy for the industry platform[8].

3 IOT TECHNOLOGICAL FRAME WORK

IOT services are possible through the implementation of different architecture and technologies. In this section we will look on different technologies used to make the IOT a reality and areas of application which are making difference in our lives.

3.1 Radio Frequency Identification (RFID)

RFID systems are important part of IOT, it consist of RFID tags and a reader. Tags contain the specific identifiers and reader reads the tags in nearby areas and sends information about different entities to central location, it is processed for further actions. The tags contain the information saved in micro embedded chip into it. When the object containing information in tags come in the range of a reader it information fetches and send to the connected system to deal accordingly. Like a vehicle with RFID tag for road tax pay pass through a reader, it read the information in tag and sends it to connected system and decreased to certain amount from the account of that specific vehicle's tag. This RFID system is one of the very first data collection systems in the whole IoTs setup.

3.2 Wireless Sensor Network

In WSN a variety of sensor nodes are installed to collect information to related objects. These sensors needs continue power supply mostly in the form of batteries and the communication link to transfer the collected information. These sensors include IP cameras, heat sensors, weight sensors, light sensors and so on. Collection of data through these sensing devices is real time and accurate. On the other hand data collected and entered by humans may cause some errors and entering the data may also lead to some errors. Network connectivity provides the smooth transfer of data the next procedural place. These sensors are core of data collection system, because all data collection is done by these sensors and then any kind of further action of processing and storage can be done, if data collection is timely and accurate, further action would also be in right direction.

3.3 Internet Connectivity

This world is now known as connected termed as global village. This all is possible through internet connectivity. In IOT after data collection its transfer is possible by using internet links may be wired but mostly wireless e.g. Wi-Fi, 3G, 4G technologies. Devices are recognized by IP address which always be unique. In present time the IPV6 addresses are in use. Before this IPV4 in use because of increase in the internet connected devices in this era of information technology IPV4 address range suspect to be short in future. To handle this upcoming problem about the addresses to be available, IPV6 is introduced which is 128bits address and capable to maintain all the devices in future.

3.4 IOT Middleware

Data presentation to user should be platform independent and have no concern to technology issues. This all is possible by the IOT middle layer, where all the technical issues have been handled by the business logic applications. The user actually unaware of process behind connectivity of things.[12,15,16] User may use different platform and the provider may be different but both should be able to communicate. It is possible through proper hardware and software platforms and middle layer in this structure at the back end provide all the necessary conversions and technical issues handling, so the user always able to get services seamlessly. All over the world IOT is deployed to solve the most pressing issues. Connected technologies are in used and increasing day by day to improve the service delivery. With the decline in cost of microprocessor and sensors, it is improving the use of IOT services in real world. Now the world is most connected then past, while 90% of the global population is covered by mobile cellular network. Now a day new technologies like 3G, 4G and other long range of technologies providing facilities for fast data communication. New and dynamic web languages and protocols like SOAP, COAP, XML and JSON becoming more popular transfer methods/mechanism for IOT.

3.5 Third Party Clouds

Among all other elements of existing architecture, clouds are also one component playing a vital role of data storage and processing by providing the pay par user service in very reasonable price. As it normal in Internet of things to collect the data continuously, to store and process this data we need resources in terms of storage devices and pro-

cessing machines. In the existing architecture of IoTs most of the services of storage and processing are carried out through third party clouds. There are many renowned and less known clouds are in existence, providers always tradeoff between the data type , its usage , user type and the price they have to pay to select the cloud setup to be used.

4 Major Challenges To IOT

Where there are huge opportunities for businesses in IOT sector and related service, there are some critical areas of concern are also present. Basically, IOT is not a conventional network technology due to its mobility and scalability and its requirement for security and user privacy are also different. In this scenario we have to secure the network and data as well as data transmission to maintain the user privacy. For example information security, user privacy, network security, sensors security and big data in IOT. In this paper our major focus on user privacy which is closely bounded with information security.

4.1 Information Security

Now day physical things are tightly bounded through wireless sensor network (WSN) with information networks. WSN is more exposed to security threats because unguided/wireless media is more open for viruses and other security attacks as compare to guided media. In IOT environment user needs availability, integrity, confidentiality and authentication. These elements are never compromised as IOT applied to crucial applications in real world like defense, medical, transportation and many more [13].

In this type of structure where things are connected through wireless connections, huge data collection and processing takes place concurrently and through link ability. Here is more chance of security attacks like DOS attacks, unauthorized access, session attacks, brute force attacks, cloning attacks, routing attacks and social engineering .These types of attacks are major concern for information security in IOT related business.

4.2 User Privacy and Trust

Privacy is not a modern term; it has deep roots science the inception of mankind. In IOT privacy defined “Privacy is the right of individuals to determine for themselves when, how and what type of information about them is collected, processed, transferred and disseminated. In IOT the actual problems arise related to user privacy is because the lack or very less control of user over the data being collected and processed. Following the taxonomy of privacy by SOLVO, privacy threats are raised during data collection, data processing, data dissemination and intrusions. [20]

In IOT environment data collection is happing on a very large scale and most of it is collected through sensors. Some sensors are located in user premises and others are not. Users may have the better control over the collection of data through the sensors within their premises but have no such choice about the ubiquitous sensors present around them in the real world and out of their own premises e.g. surveillance cameras. The collection of such huge data and its processing, father more its transfer and presentation is the major source of user privacy threats. During all these phase’s data is collected through sensors and it is transferred through wireless network and stored on the centralized cloud storage and furthermore link ability of the all transaction from a user makes it more vulnerable to user privacy. [17]

A client may need privacy from network owner and the provider also. In IOT networks the most important threat to user privacy is tracing user by linking transaction and queries from a particular user using different devices and services. User needs privacy regarding to its location as well as about its queries for using the services. This is possible by making the customer anonymous in the WSN. This will help the user to maintain its privacy. This will also make it possible to save the user form the profiling and traceability of user’s transactions. When user is anonymous than transactions from a particular user are not linkable or traceable. This capacity of unlink ability make the privacy of user enhanced and strong than previous.

4.3 Limitations of embedded devices

Firstly, embedded device like sensors and other smart devices need to be energy efficient to make the device work for a longer time. To achieve this goal we have compromise on its storage and processing capabilities and just focus on its primary function just to collect data, not to store or process it and pass it on to next level after collecting it from the place or environment where it is installed. This limitation lead us to communicate data to the next level through wired or wireless medium and if is wireless it farther leads to certain security threats attached with wireless environment. Secondly, physical security also matters due to mobile nature of embedded devices and the unsecure physical location may cause security concerns.

4.4 Cloud and third party participation

IoT is one of the source of Big Data, through the sensors huge amount of data have been gathered and need to process and store for use of in different kinds of analysis[5,25]. So in IoT it is normal to involve the third party services such as private clouds and such other setups to store and process such huge amount of data. Meanwhile it is normal practice to take services like “pay per use” from clouds and third parties. This approach may lead us to compromise upon customer’s private information due to storage out of provider’s premises and one of the major problems is data transmission from provider to clouds and other locations. User may not be informed about the use of his personal information and in the future is user found any misuse of his/her personal information than surly lose the confidence in such type of services which is not good form future of such networks [2].

5 Our Contribution

During literature review and study of ongoing and previous research of problem areas and their solutions we found that if

two major issues get settled, many of the problems according user privacy would be solved. Firstly, by minimizing data storage and processing on clouds and third parties setup. In future providers of such ubiquitous services should focus to enrich their hardware setups in term of data storage and processing so that they can store the real time and sensitive information about user that can be harmful if got hacked and have to depend on third party services only for archives and non sensitive data storage.

Secondly, by making some more efforts to keep information secure during transmission from sensors to providers and from providers to third party (non sensitive data). This could be done by making standards of encryption more efficient by making combination of public private key encryption rather than only public key encryption (as in previous approaches) and continuous change in the keys. This solution is appropriate when we are collecting data from sensors because some specific limitation of remote devices in term processing but when transferring the data from controllers to provider and then to cloud and third parties this will be applicable and going make difference. By this maximum information security can be ensured and this will enhance the user privacy which is our main focus.

6 Conclusion

IOT is relatively new field of technology and have been adopted in some selected countries. IOT has the bright future opportunities to be spread all over the world into different fields. There are major concerns are present in term of its security and user privacy as mentioned by most of the researchers. In presence of these threats user would not be confident to adopt these services and IOT will not flourish with rapid speed. By taking measures to counter security and privacy threats as suggested in this paper to enhance the providers premises in term of processing and storage than depends on clouds and third parties. Secondly by adopting better information security measures as public private key combination, continuous change and improvement with the passage of time also improve the security during the communication of personal information. By taking all these actions user privacy will improve and user would be more confident to adopt these kinds of devices. This will enhance the future of things to things connectivity. There are many open issues for researchers to make the things standardize in term of security and architecture to be used in IoTs, solution of such issues also enhance the use of IoTs in near future.

References

[1] Chen, D., Bovornkeeratiroj, P., Irwin, D., & Shenoy, P. (2018, July). Private Memoirs of IoT Devices: Safeguarding User Privacy in the IoT Era. In Proceedings of the 38th IEEE International Conference on Distributed Computing Systems (ICDCS'18).J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Bertino, E. (2016, March). Data Security and Privacy in the IoT. In EDBT (Vol. 2016, pp. 1-3).

[3] Zhou, J., Cao, Z., Dong, X., &Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: challenges. IEEE Communications Magazine, 55(1), 26-33.

[4] [4] Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11).

[5] Ukil, A., Bandyopadhyay, S., & Pal, A. (2014, April). Iot-privacy: To be private or not to be private. In Computer Communications Workshops (INFOCOMWKSHPS), 2014 IEEE Conference on(pp. 123-124). IEEE.

[6] Gan, G., Lu, Z., & Jiang, J. (2011, August). Internet of things security analysis. In Internet Technology and Applications (iTAP), 2011 International Conference on (pp. 1-4). IEEE.

[7] J.Shao,H,Wei,Q,Wang and H.Mei 'A runtime model based monitoring approach for cloud, In cloud computing' (Cloud) IEEE 3rdInternational, 2010.

[8] Keith D.foote. "A Brief History of Internet of things" Internet: http://www.dataversity.net/brief-history-internet-things, August 16, 2016. [May 25, 2017].

[9] Rajnish Kumar, Information & Communication Technology, Operations Research, 2102. Internet: www.audIOTech.com/trends-magazine/articals, 2014.

[10] Charles McLellan, 'The Power of IOT and Big Data, There are few of the application areas of IOT and their overview is given' March 2, 2015.

[11] L.Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survay, Computer Network' Vol. 54, pp. 2787-2805, 28 October, 2010.

[12] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, 'Convergence of MANET and WSN in IOT Urban Scenarios' IEEE Sens. J.Vol.13.No.10,pp.3558-3567. Available: www.postscape.com/internet-of-things-history [Oct, 2013.]

[13] OrgeLanza , Luis Sánchez , Verónica Gutiérrez, José Antonio Galache, Juan Ramón Santana, Pablo Stores and Luis Munoz, Network Planning and Mobile Communications Laboratory, University of Cantabria, Spain, Received: [17 May 2016] Published: [6. September,2016] Available: ieeexplore.ieee.org/ieln7/6488907/6810798/06740844.pdf

[14] Hemant Ghayvat,Subhas ukhopadhyay, Xiang Gui and Nagender Suryadevara, SEAT, Massey University, Palmerston North 4442, New Zealand.

[15] C. Tein-Yaw, I. Mashal. O. Alsaryrah. C. Chih-Hsiang, H. Tsung-Hsuan, L. Pei-Shan. ET. Al. 'MUL-SWoT: A Social Web of Things Platform for Internet of Things Application Development'.2014 IEEE International Conferences on Green Computing and Communications, IEEE. 2014, pp. 296-299.

[16] A. Sanchez Pineda, Maranoon-Abren, R. (2014). Like Art: 'Integrated Internet of Things and Social Networks'. Available: www.like-art.com.

[17] Z. Yu, W. Jiangtao, and M. Fan, 'The Application of Internet of Things in Social Network, in Computer Software and 38th International, 2014, pp. 223-228.

[18] WOOD. A.D. and J. A. Stankovic. 2002. 'Denial of Service in Sensor Networks'. IEEE Computer, 35(10), 54-62.

[19] Arijit Ukil, Soma Bandyopadhyay and Arpan Pal, 'To Be Private or Not to be Private' IEEE, 2013.

[20] Elisa Bertino, 'Data Security and Privacy in IOT' Department of CS, Perdue University West Lafayette, 15 Aug 2016.

[21] Biego Mendez, ioannis papa pauagou, Baijian yang, 'IOT: Survey on Security and Privacy' University Perdue, 10 July 2017.

[22] Cristina Alcaraz, Pablo Najera, Tavier Lopez, Rodrigo Roman, 'WSN and IOT, Do we need a Complete integration' University of Malaga, Spain, 2011.

[23] 'IOT a survey on enabling technologies, Protocols and applications.' IEEE Communication Surveys and Tutorials. Vol.17, No.4, Fourth Quarter, 2015.

[24] Muhammad A. Iqbal, Oladiran G. Olalaye and A. Bayoumi, 'A Review on IOT : Security and Privacy Requirements and Approaches' University of Louisiana at Lafayette, 2016.

[25] Jan Henrik Ziegeldorf, Oscar Garcia Morchon and Klaus Wehrle, 'Privacy in the Internet of Things: Threats and Challenges' Communication and Distributed Systems, RWTH Aachen University, Aachen, Germany

[26] Philips Research, Eindhoven, Netherlands.Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies. (2015, January) Security in Computing, (5th Edition).