KALAM – International Journal
Faculty of Arts and Culture,
South Eastern University of Sri Lanka.
14(4), 2021

Security breaches on Individual's Privacy via Internet of Things Applications

Ahamed Sabani, M.J.[1], Shafana, M.S.[2] & Zisath Shama, L.F.[3]
[1, 2, 3] Department of Information and Communication Technology
South Eastern University of Sri Lanka

Correspondence: mjasabani@seu.ac.lk[1], zainashareef@seu.ac.lk[2], shamalfz@seu.ac.lk[3]

Abstract

The Internet of Things is an organized structure of objects which are able to interact between themselves. IoT mainly resides in data collection and collaborates with several technologies and entered deeply in daily human life Moreover, it requires cloud computing services, robust inter-network connectivity, secure data storage, processing, and analytics for enhanced advantages. IoT connects the devices using mostly Wi-Fi networks and sensors. An analytic survey says that in IoT, the number of connected devices is growing each year significantly. In the sense of data collection, there are some risks and threats to an individual's privacy. Security and privacy are primary elements to be considered in IoT. Through this study, some significant themes of privacy were identified related to gathering personal information through IoT technology such as unauthorized surveillance, inadequate authentication, information security risks, and uncontrolled data generation and usage. Reduction of privacy is unavoidable with IoT technology because of the increased collection of data, which causes some issues for each individual such as spying, information diffusion, disclosure of the collected sensitive data, problems of security, and hacking of the gathered data. These kinds of security problems can be sorted out by providing secure logins to increase the individual's trust of IoT technology, by developing and establishing the individual's anonymity for effective use, by using encryption techniques, by implementing adequate security protocols for sensor use.

Keywords: Data Security, IoT, IoT collaborative technologies, IoT devices, Privacy issues.

Introduction

The Internet of Things (IoT) impacts significant factors of human life Health, house, fitness, security, facilities and equipment, interaction, industry, transport, education, government, scientific, mankind, commercial and emergencies. IoT is a rising structure of physical devices, integrated with actuators, sensors, software, control systems, automation, able to communicate with each other, to monitor the environment, to broadcast collected data. IoT can be an accelerator of the right to access knowledge. Today with the emerging technical architecture related to the internet, IoT is a major disruptive technology (Gubbi et al., 2013; Weber, 2010). Meanwhile, the internet is a physical architecture constructed by using routers, switches, firewalls, computer-related devices and other networking equipment. The World Wide Web (WWW) service is running on the internet to provide resource sharing facilities. In the concept of IoT, we are extending the connectivity beyond the conventional computer

network through the internet using WWW services. It means the objects or devices will be connected with the IoT system. Moreover, it will provide the ability to transfer data over the network automatically using very less human interaction. IoT offers new personalized and reality augmented services for the organizations and third parties to collect and analyze the environment's as well as individuals' attributes (Vermesan et al., 2011). The adoption of IoT technology increases as the government and more organizations prioritize digital transformation. The following statistics show the continuous expansion of IoT technology.

According to one of the IoT analytic site, the number of connected devices is growing significantly. It shows an unexpected acceleration in the year 2018, and it exceeds 7 billion IoT devices, excluding smartphones, tablets, laptops and fixed-line phones (Lueth, 2018). Fig. 1 shows the progress of IoT devices connected in the past, and the expected growth in future. This analysis had been done in the year 2018, and according to their expectation, the number of connected IoT devices would have reached only to 8.3 billion in the year 2019. Nevertheless, in fact, it has been exceeded to 26.66 billion in the year 2019.

Moreover, the statistics say that, 127 new devices being connected to the web every second. Experts estimate that the installation of IoT devices to Worldwide would be drastically increased to 31 billion, 35 billion and 75 billion respectively in the year of 2020, 2021, and 2025. Likewise, the prediction says that IoT technology may be adopted by 93% of enterprises and 80% of industrial manufacturing companies in the world by the year 2020, and also 90% of cars and 3.5 billion cellular IoT would be connected to the web through IoT (*The IoT Rundown For 2020: Stats, Risks, and Solutions*, 2020).

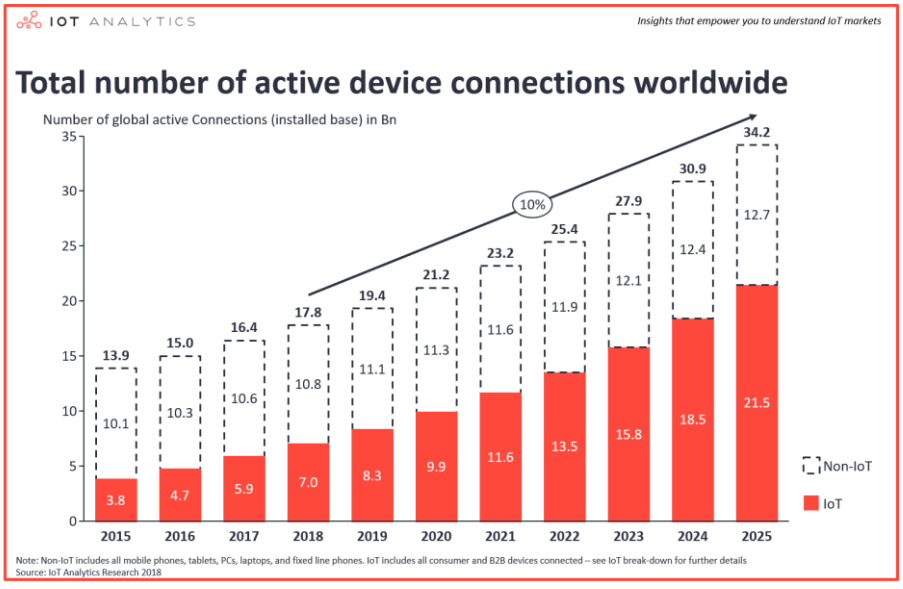

Fig. 1: Total number of active device connections worldwide (iot-analytics.com)

Several collaborative and communication technologies are integrated into the process of IoT for their task of comprehensive data collection. Besides, to enhance the advantages of IoT, it requires cloud computing services which facilitate the data transmission, processing and analytics (Abdul Rahman et al., 2016). Moreover, to create a global network, IoT uses cloud computing and robust inter-network connectivity to connect the devices with efficient data sharing method, and secured data storage. IoT connects the devices using mostly Wi-Fi networks and sensors.

Several types of sensors are used in this field to collect data. Camera (CCTV) used to record the movement and facial identification, which can be used in crime investigation. Smartwatch to record the vital signs, movement and voice recordings can be used in healthcare. Google glass used to record surroundings and movements which can be used in improved marketing interaction. Building sensors used to record movement, heat and consumption (water, power, and internet) which can be used in the Energy industry. Smartphone used to record the call history, location, movement and internet/app activity to use for crime investigation and fraud. Goods packaging used to track delivery, quality control and real-time inventory in the retail industry. Human implants used to monitor blood pressure, location, and heartbeat, which can be used in healthcare. Moreover, vehicle to record movement, driver behaviors, fatigue/alcohol, and traffic reduction, which can be used in consumption savings and accident prevention (Atzori et al., 2010; Caron et al., 2016; Stanford, 2003). Such the above ways, IoT involves in everyday lives of individuals and society.

Nowadays, human lives have been addicted to the IoT for most of daily life. A typical healthcare industry uses a central cloud-based system which contains the data of patient medical report and wellbeing. Medical professionals can access this data to examine the patient's health condition. When we see in the qualitative economic standpoint, ICT applications communicate with the physical world. Furthermore, it is providing an ample chance to achieve liquid marketplaces, allowing industries, and processes to integrate IoT devices to technology-intensive. Even in developing countries, IoT may provide Multi-Factor Productivity by providing easy access to ICT to both general population and industries.

Mobile Medical Apps are widely used in IoT to provide pervasive health. According to an industry survey, more than 1.7 billion smartphone and tablet users might have downloaded a Mobile Medical Apps by 2018. These apps work on sensitive data and often controls physiology. Moreover, it is as an opening for innovations and providing low-cost healthcare delivery for all of us. In the sense of interconnectivity as a computer network or an IoT system, Security and Privacy are primary elements to be considered. There are many protocols, and security mechanisms have been invented and updating them very frequently. Even though most of the services are assuring privacy, we cannot fully trust, because those systems can be compromised with the latest technology that we have. Thus, it will be an arguable topic.

Therefore, there is an extreme significance in the study of different security problems in IoT. The main objective of this study is to literature the issues of Internet of Things on a survey purpose.

Literature review

Multiple stakeholders involve into the IoT procedures in an information privacy perspective. They are individuals from whom the data is going to be collected, organizations who have the responsibility to process the individuals' gathered data, and third parties who get benefit from data. All these three stakeholders are getting benefit from the IoT. Individuals are getting healthier and comfort benefits. Organizations and third parties are providing information to deliver highly improved services to people and the community heavily. Though, when we considering the increased collection of more personalized data of individual from a legal perspective, IoT data collection causes some impacts on individual's privacy.

Literature (Weber, 2010) highlights that IoT's purpose is to facilitate secure and reliable exchange of information about 'things', 'Secure' and 'reliable' are the key factors that impact on individual data protection privacy, particularly during the unintentional and ethical use of gathered IoT data, and the access of third-party users.

The increased collection of data causes some issues on individual's privacy, such as tracking people's movements and behaviors encourages spying (Abowd & Mynatt, 2000; Kindberg & Fox, 2002). Preparing extensive data set using data mining technique could encourage surveillance technique which allows finding the individuals' behaviour (Atzori et al., 2010; Satyanarayanan, 2001). The authors of (Čas, 2005; Jiang & Landay, 2002; Stanford, 2003) conveyed that reduction of privacy is unavoidable with IoT technology.

The collected data need to be trustfully handled (Beresford & Stajano, 2003; Čas, 2005; Weber, 2010). Literature (Atzori et al., 2010) says that it is almost impossible the control of the information diffusion because of the web application and sensors. Data handling is linked with some regulations such like the limit on the use of sensors, obligations towards the customer and the legislation, authorization to disclose the collected data (Baldauf et al., 2007; Weber, 2010), transparency policy for end-users to ensure that rules and regulations.

In terms of access control, centralized service authentication is not enough to provide sufficient security (Haller et al., 2009). Automatic identification also leads to some new risk (Oriwoh et al., 2013).

It must provide secure logins to increase the individual's trust of IoT technology. There should be some ways to develop and establish the individual's anonymity for effective use of IoT (Beresford & Stajano, 2003). Also, there are some problems of security and hacking of the gathered data by multiple and collaborative connected devices on IoT (Vermesan et al., 2011). These kinds of security problems can be shorted out by using encryption techniques (Abowd & Mynatt, 2000; Campbell et al., 2003; Chan & Perrig, 2003; Gubbi et al., 2013). Moreover, most of the sensors are not able to provide adequate security protocols due to their minimal size and power consumption (Chen, 2012).

Methodology

Sources for this study were referred from multiple databases. Initially, to create a shortlist of peer-reviewed articles, searched in Google scholar by applying broad terms. In the beginning, we travelled over a simple search of "issues in the Internet of Things". From the research paper titles derived from the initial seek, it was able to use an extensive list of sophisticated terms when retrieving from other databases. Through the Universities' digital repositories of libraries, we had a limited search to catch the conference papers allied to our topic. The search terminologies were chosen for this literature survey comprised of security issues, IoT loopholes, disadvantages of IoT, dissatisfaction in IoT system, attacks on IoT, privacy issues and other related keywords. These terms were gathered in various ways with "AND" conjunction to locate the clarified related articles.

Most of these searched keywords were formed from the outputs of the primary search and merged with results from the various academic repositories. Each of the keywords utilized because of their fitness and relevance with the aim of this research. Chosen sources were examined based on a set of criteria. First, the retrieved articles had to be within the boundary of the objectives of this study.

Discussion

Despite the immense welfares the users are enjoying from the IoT, some risks come along with it that essential to be shorted out. Privacy risks and cybersecurity are the leading concerns that have been mentioned. These two are causing an enormous predicament for many organizations. Predominant high-profile attacks in cybersecurity have revealed the vulnerabilities of IoT technologies.

Most IoT end devices are constantly connected to the Internet and are usually with naive security configurations. Leveraging vulnerabilities on a device, adversaries can control the device remotely. Most of the cybersecurity professionals think IoT applications as an important loophole for cyber-attacks due to its weak security policies and protocols. Meanwhile, some inappropriate security practices of users lead to cybersecurity risks and access to malicious applications which pay a pathway to increase the data breaches of sensitive data and other threats. There are some practices of users which are most pressing vulnerabilities such insecure password, using unneeded or insecure network service, insecure ecosystem interfaces, using insecure or outdated components, insecure default device settings, lack of physical hardening and device management. Most of the users apply guessable, weak and hardcoded passwords as because of their easiness. Usage of these passwords leads to unauthorized access because it can be guessed easily; thus, these are generally simple, short and most publicly available one.

Furthermore, insecure network services which are installed on users' device would expose financial and sensitive data to eavesdropping and theft. Also, the insecure external interfaces may compromise the devices and their components to threaten the existing system. Some users are eager to use some components such as third-party and open-source, which were not scanned for vulnerabilities. Moreover, the inability of the user to fix insecure settings may lead to loopholes in devices and systems. Likewise, the lack of physical hardening allows threat actors to take control of the user device or system, which causes a larger attack surface. In the case of security breaches, not only the user side but also the service providers take part like producing the device with lack of security mechanism and update, insufficient privacy protection, and insecure data transfer and storage. There are security mechanisms which allow unencrypted data to move from unauthorized sources towards the device by applying inadequate security monitoring. IoT devices have a storage facility to necessary information within it. Some IoT devices fail to protect such sensitive private information which is stored on the IoT devices and connected ecosystems.

As it is discussed above, IoT modules make trouble the security boundary. The more IoT components we attach to the network, the more attack surface we add to the network. There are three main ways to a network from the Internet of Things such as Monitor endpoints, continuous scanning on devices for vulnerability, and creating a dedicated Internet of Things network. Endpoint Detection and Response (EDR) tools in cybersecurity can be forced to protect the network. The endpoint of a network can be monitored through the EDR tools and also look for threats and send security alerts.

Furthermore, not only by scanning the devices before enabling the connection with the network but also by a continuous scanning on vulnerability can ensure the unceasing health of the network and its components. Controversy, networks can be secured by keeping it separated from IoT components. For this purpose, the wireless network can be dedicated to IoT, and this network should have access to the internet but not to the cooperate network (*The IoT Rundown For 2020: Stats, Risks, and Solutions*, 2020). Moreover, several factors and concerns might have an impact in the case of securing the Internet of Things devices such; the security patches should be updated by the IoT manufacturers and in Operating System (OS) versions in a frequent, occasional manner before the hackers get sufficient time to blow the

security protocols and rob the sensitive data; embedded password which helps the technicians to troubleshoot problems and install updates remotely should be secured without could be utilized by the hackers to penetrate the security of the device; Automation property of Internet of Things system has been used by the enterprises and end-users for data gathering or simplifying activities. However, if the malicious sites are not specified, integrated Artificial Intelligence may access such sources which could allow threats to arrive into the system; IoT components employ various network protocols for remote access such as ZigBee, Wi-Fi, Z-Wave. Usually, specific limitations are not declared, which may be used to avoid cybercriminals. Therefore, hackers could quickly launch a malicious connection via these protocols for remote access. Thus, remote access protocols should be established by considering these loopholes; several third-party software applications exist on the Internet to perform several specific operations. If the users install or access such applications, hackers will easily and automatically enter into the IoT system and spoil the embedded database. These kinds of problems can be resolved by making the authenticity of these third-party applications could be identified easily and restricting or limiting the network threats; Normally, IoT manufacturers design unique device identifiers to track and monitor them. Still, certain manufacturers keep weak security policies for these purposes. Consequently, detecting distrustful online deeds become quite problematic. Thus, IoT manufacturers should sustain with adequate security policies to configure unique IoT devices (Tawalbeh et al., 2020).

By the development of more sophisticated security functionalities and implementing these features into IoT products, hacks could be avoided. This prevention is because the end-users will purchase IoT products that already hold adequate security functionalities blocking vulnerabilities. Cybersecurity mechanisms are some of the steps to put forward to guarantee that IoT is secured.

Conclusion

IoT includes imaginable objects and devices that are connected to a smart device to gather, share data and communicate over the internet. When collecting and handling personal data in an IoT system, there are some risk and threats to an individual's privacy. Through the literature review, some significant themes of privacy were identified related to gathering personal information through IoT technology such as unauthorized surveillance, inadequate authentication, information security risks and uncontrolled data generation and usage. While some service providers giving a guarantee of privacy for individual's data, there were some pieces of evidence for security breaches. In future, not only the IoT technology should emerge the techniques which can be used to solve the privacy issues on individual data to enhance the advantage of IoT technology and the projects but also the users should have the concern to overcome the problems which can be resolved in the user side.

References

Abdul Rahman, A. F., Daud M., & Mohamad M. Z., (2016). Securing sensor to cloud ecosystem using Internet of Things (IoT) security framework. *ACM International Conference Proceeding Series*, *22-23-Marc*. https://doi.org/10.1145/2896387.2906198

Abowd G. D., & Mynatt E. D., (2000). Charting Past, Present, and Future Research in Ubiquitous Computing. *ACM Transactions on Computer-Human Interaction*. https://doi.org/10.1145/344949.344988

Atzori L., Iera A., & Morabito G., (2010). The Internet of Things: A survey. *Computer Networks*. https://doi.org/10.1016/j.comnet.2010.05.010

Baldauf M., Dustdar S., & Rosenberg F., (2007). A survey on context-aware systems. *International Journal of Ad Hoc and Ubiquitous Computing*. https://doi.org/10.1504/IJAHUC.2007.014070

Beresford A. R., & Stajano F., (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing*. https://doi.org/10.1109/MPRV.2003.1186725

Campbell R., Al-Muhtadi J., Naldurg P., Sampemane G., & Mickunas M. D., (2003). Towards security and privacy for pervasive computing. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/3-540-36532-x_1

Caron X., Bosua R., Maynard S. B., & Ahmad A., (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2015.12.001

Čas J., (2005). Privacy in pervasive computing environments - A contradiction in terms? *IEEE Technology and Society Magazine*. https://doi.org/10.1109/MTAS.2005.1407744

Chan H., & Perrig A., (2003). Security and privacy in sensor networks. *Computer*. https://doi.org/10.1109/MC.2003.1236475

Chen Y., (2012). Challenges & Oppoetunities in IoT. *IEEE Conference on Wireless Sensors (ICWiSe)*, *16*(12), 383–388.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2013.01.010

Haller S., Karnouskos S., & Schroth C., (2009). The Internet of things in an enterprise context. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-00985-3_2

Jiang X., & Landay J. A., (2002). Modeling privacy control in context-aware systems. In *IEEE Pervasive Computing*. https://doi.org/10.1109/MPRV.2002.1037723

Kindberg T., & Fox A., (2002). System software for ubiquitous computing. In *IEEE Pervasive Computing*. https://doi.org/10.1109/MPRV.2002.993146

Lueth K. L., (2018). *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating*. IoT Analytics. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Oriwoh E., Sant P., & Epiphaniou G., (2013). Guidelines for Internet of things deployment approaches - The thing commandments. *Procedia Computer Science*. https://doi.org/10.1016/j.procs.2013.09.018

Satyanarayanan M., (2001). Pervasive computing: Vision and challenges. In *IEEE Personal Communications*. https://doi.org/10.1109/98.943998

Stanford V., (2003). Pervasive computing goes the last hundred feet with RFID systems. In *IEEE Pervasive Computing*. https://doi.org/10.1109/MPRV.2003.1203746

Tawalbeh L., Muheidat F., Tawalbeh M., & Quwaider M., (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences (Switzerland)*, *10*(12), 1–17. https://doi.org/10.3390/APP10124102

The IoT Rundown For 2020: Stats, Risks, and Solutions. (2020). Secutity Today. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2

Vermesan O., Peter, F., Patrick G., Sergio G., Harald, Sundmaeker Alessandro B., Ignacio Soler J., Margaretha M., Mark H., Markus E., & Pat D., (2011). Internet of Things: Strategic Research Roadmap. In *Internet of Things-Global Technological and Societal Trends*.

Weber R. H., (2010). Internet of Things - New security and privacy challenges. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2009.11.008