IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 9, June 2022

Pursuit of Privacy in the IoT Domain

Lekha Mangesh Naik
Student, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *The massive web of linked devices and people i.e. "The Internet of Things" (IoT) has become an inevitable segment of all demographics in today's era. With current revolutions in "Industry 4.0", the world is predicted to cater to 64 billion IoT devices by 2025. While consumers relish the "smart of everything" offered in the market, their privacy concerns remain an issue of critical importance. "Online Privacy" of an individual has been a debated matter of interest since the advancements in social media, and with the prevailing developments in the IoT sector for making consumers lifestyle effortless, the volume and variety of personal data gathered is humongous. This collected data of consumers if leaked or used in an unethical manner by businesses can result in privacy threats. This paper addresses various threats and repercussions to consumers that exist through the applications and devices of the IoT world. Further, the paper analyses whether the consumers are well-aware about how their information is being recorded and the extent to which their personal data is shared by them to the businesses and the consequences that can arise to their data. The paper ends with solutions in favour of these consumers to ensure that they are well acquainted with the privacy policies and threats that abide with these devices they use.*

Keywords: Internet of Things, Industry 4.0, Fourth Industrial Revolution, Privacy, Online Privacy

I. INTRODUCTION

Access and usage of individuals' data by businesses and service providers have been a long-debated privacy concern till date. Now, with the emergence of IoT devices that monitor and record all of users' details, preferences, locations, etc., these devices being connected to the internet throughout, maintaining online privacy of users all along and keeping user's data safe from hackers or limited use of data to permissible extent by service providers is the ultimate concern to the privacy of consumer.

1.1 Privacy

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [1]. Privacy involves the policies, procedures, and other controls that determine which personal information is collected, how it is used, with whom it is shared, and how individuals who are the subject of that information are informed and involved in this process [2]. Westin has defined four states of privacy viz. Solitude, Intimacy, Anonymity and Reserve for describing the concerns of individuals regarding the security of their personal information from others. Solitude means individuals choice to be separated from the group and freed from the observation of other persons; Intimacy states that individual is part of a small unit; Anonymity means individual is in public but still seeks and finds freedom from identification and surveillance; Reserve is the creation of a psychological barrier against unwanted intrusion - holding back communication [1]. Similarly, Solove's Privacy Taxonomy regarding person's information safety states the following - Information Collection including Surveillance and Interrogation for acquiring individuals data; Information Processing consisting of Aggregation, Identification, Secondary Use of data collected from user for further usage and implication through it; Invasion having Intrusion and Decisional Interference relating to violation of user's data and; Information Dissemination concerning Breach of Confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation, Distortion indicating various infringements concerning threat to consumer's vulnerable data[3].

1.2 Internet of Things

A network of physical and virtual things on a global scale wherein every object holds a unique ID where all electronic devices communicate within each other constitutes the concept of IoT. Here, since most devices are battery dependent,

DOI: 10.48175/IJARSCT-5420

implementing security and privacy mechanisms is an issue owing to the constraint of minimal processing power. Hence, addressing major challenges in IoT pertaining to authentication, identification and heterogeneity amongst devices becomes an issue [4].

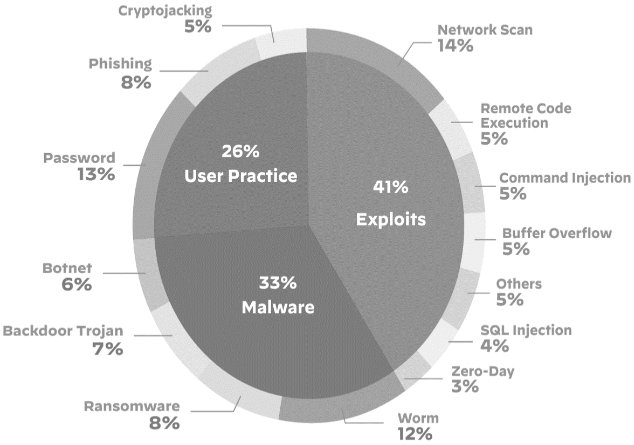

Fig. 1 Major IoT Threats

Most prevailing threats to security in IoT are depicted in Figure 1. Device vulnerabilities are being targeted through exploits which include attacks through network/ IP/ port/ vulnerability scans on networks for finding targets. Furthermore, attacks due to negligence of the health of passwords enables attackers to break into devices gaining access into the heavily interconnected environment of IoT. IoT worms for spreading malware in networks and IoT botnets for implementing DDoS attacks through IoT devices are other prominent attacks [5].

1.3 Fourth Industrial Revolution

The most recent technological revolution i.e., Industry 4.0 aims to provide a linked and smart manufacturing system where web, system and personage would be massed together, and its concept of implementation is entirely focused on information created from data exchanged amongst devices and machines [6]. This mechanism results in exposure of the utmost private information of users. Industry 4.0-based businesses have large reliance on data which leads to cybersecurity concerns and needs and advancing cybersecurity perspective [7]. Technologies like cloud-based systems, Big Data, BYOD (Bring Your Own Device) and CYOD (Choose Your Own Device) are set as trends with the emergence of this revolution. Although, these advancements have led to new loopholes in cyberspace creating threat to consumers' data which are at times neglected by businesses to achieve outsmarting benefits [8]. In this era of Industrial Internet of Things (IIoT), with the huge number of devices being involved in interchanging data through open channels, security and privacy concerns need to be addressed with higher level of cryptographic solutions to ensure integrity and authenticity [9].

II. LITERATURE REVIEW

A notable work in analysing the familiarity of information disclosure through online platforms and its security inferences is done in the paper "Information Revelation and Privacy in Online Social Networks (The Facebook case)" by Ralph Gross and Alessandro Acquisti wherein they studied online conduct of more than 4,000 students to assess the quota of data revealed and noticed the utilization of privacy settings whereof it was noted that only bare minimum of users change the extremely penetrable privacy preferences [10].

"Privacy in India: Attitudes and Awareness" by Ponnurangam Kumaraguru and Lorrie Cranor is another noteworthy research in which they have done an investigative study with regards to analysing degree of consciousness referring to privacy-related concerns in educated persons in India which resulted into noting gross deficiency of recognition of privacy issues and negligence of privacy in India as compared to results of identical study done in the United States [11]. Ponnurangam Kumaraguru and Niharika Sachdeva in the further version "Privacy in India: Attitudes and Awareness V 2.0" state that Indian citizens were so oblivious about the Government with regards to their privacy, they were deceived by the mindset to believe they are protected by privacy laws although there are no privacy laws implemented in India [12].

A valuable insight can be drawn from the paper “Privacy and the Internet of Things: Emerging Frameworks for Policy and Design” by Rosner Gilad and Kenneally Erin where they highlight the major privacy concerns emerging due to increase in implementation and usage of IoT devices and how utilization of wearable and automation devices can be threatening to consumers’ security and privacy due to the amount of behavioural data collected and comprehensive information tracked by these devices. The paper also calls attention to the fact that consumers are failing to keep track of the manner in which the possessed information is being shared by organizations and demands necessary measures from businesses and government for the security and privacy of the data gathered from users [13].

“Privacy in the Internet of Things: Threats and Challenges”, a paper by Ziegeldorf Jan, Morchon Oscar and Wehrle Klaus, affirms that due to constant advancements in the field of IoT, the related threats keep iterating. Hence, they need to be anticipated beforehand to safeguard data security and to suffice this, synchronized actions on the technical and government front required to ensure safety of consumers [14].

To review the current IoT developing sector of Industry 4.0, Pereira Teresa, Barreto Luis and Amaral António in their paper “Network and information security challenges within Industry 4.0 paradigm” call attention to requirement of security plans and strategies by businesses in the IIoT sectors and plan of action under view by organizations to implement security measures into technological confrontations risen by Industry 4.0’s deployment into all areas keeping in consideration cost incurred to business to avail security [15].

Mentsiev Adam, Guzueva Elina and Magomaev Tamirlan in their paper “Security challenges of the Industry 4.0” bring into view that rightful execution of IIoT depends majorly on the proper safeguarding of the security issues that accompany. They also recommend measures such as creating awareness amongst the industrialists, entrepreneurs of Industry 4.0 and expressed the need to focus on the policies and allotting finances for implementing security. They also point out transparency be maintained for risk involved for the user [16].

Realization of consumers other than manufacturers is called out in the paper “Addressing Industry 4.0 Cybersecurity Challenges” by Giovanna Culot, Fabio Fattori, Matteo Podrecca and Marco Sartor as to convey safety conducts for upcoming Industry 4.0 advancements against unforeseen cyberattacks for which attention and action on global level are suggested by them to enforce cybersecurity effectively [17].

The rising prominent issue with regards to Personally Identifiable information (PII) is discussed in the paper “Personal Data Privacy Challenges of the Fourth Industrial Revolution” by M. M. H. Onik, C. S. Kim and J. Yang where they state that understanding the differentiation between the terms security and privacy is of utmost importance for deploying a secure environment for user data and convey that current rules and laws of personal information are insufficient as per upcoming advancements in IIoT [18].

III. OBJECTIVES OF RESEARCH

Determining the level of awareness in users concerning the data collected about them by their regularly used devices. Assessing the understanding and usage of privacy options by consumers for maintaining access limitations by their devices. Describing the perspective of consumers with regards to their data privacy and information security concerns and expectations from providers based on results of the study done.

IV. RESEARCH METHODOLOGY

Survey methodology was adopted in this paper for conducting study and acquiring quantitative data from users. Around 60 users of varying age groups were asked to respond to a questionnaire about data privacy and security in IoT devices. The survey consisted of 15 questions aligned around concepts of maintaining user’s information security through IoT gadgets. The responses thus obtained would help to analyze consumer’s perception of issues and concerns relating to their data privacy while utilizing these IoT devices. Surveying enables the gathering of precise statistical data and since the respondents’ range into different age brackets of consumers, the accuracy of survey results is hence more reliable. The questionnaire is designed in a manner to examine consumers' knowledge and perception about potential and probable risks to their personal information associated via use of IoT devices.

DOI: 10.48175/IJARSCT-5420

V. ANALYSIS AND FINDINGS

The evaluation of the survey results ranging over different age groups of consumers helped to analyse users' outlook towards various aspects concerning security and privacy with regards to taking initiative to safeguard loopholes on user level and anticipation towards institutions for protecting their seclusion.

Figure 2 shows feedback over maintaining preventive measures on user level while using the devices as per which it is deduced that most consumers do not bother to disconnect their devices from the network or continue to keep them in discoverable mode even when they are not in usage. This negligence on the user's part may result in allowing trespassers to gain access through network invasion or unauthorized device connectivity. Also, the survey results convey that many users, mainly ranging into elderly age group' don't change the default passwords on devices which is another concerning issue for user's privacy.

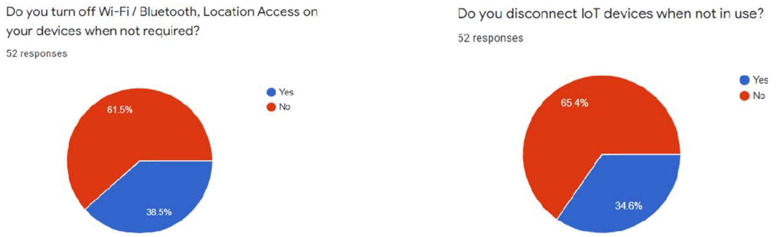

Fig. 2 User's response on implementing precautionary measures

Figure 3 depicts user's consciousness over allowing or disabling permissions on devices that permits it to access in consumer's data which as per the responses show that a greater percent of users is of those who do not pay attention to reviewing the default set access permissions which may lead to unwanted degree of data sharing. Another majorly concerning response from the survey exposed that only a negligible percentage of consumers read through the essential agreements of privacy policies which convey to users what and how much of their data they are authorizing the companies to access and the rights they permit them for further actions on the acquired data.

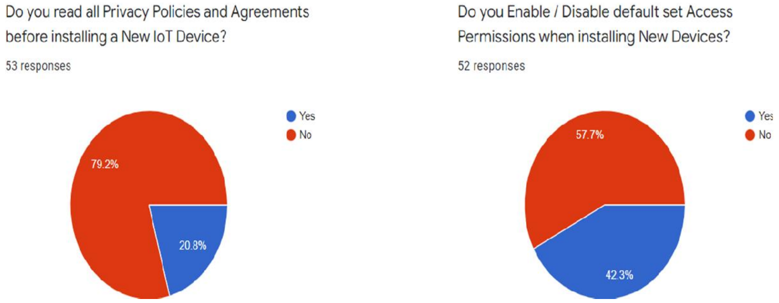

Fig. 3 User's response on granting access permissions

With regards to the concerns of data theft and misuse, the survey feedback shows that the majority of consumers fear for their personal information on this front. Whereas on the matter of being aware of the fact that businesses are able to collect private information or PII about consumers through their devices, the survey results convey that mainly users from minor and elderly age groups remain oblivious of the actuality.

Similar response is inferred mainly from these age groups as shown in Figure 4 for being unaware that businesses could use acquired data of users for manipulating consumer's decisions against their will in favour of firms for gaining sales benefits or share consumer's personal data to third parties in exchange of monetary benefits which would result into an extreme threat to consumer's privacy and security.

Consumer's response for the survey question about necessity of genuine feasible disclosure can be seen through Figure 4 wherein maximum users desire to get transparency from the businesses as to what data of consumer's is being gathered and their rights over the collected data for sharing and processing. Also, absolute responses in survey results are seen for demand of enforcement of rules and regulations from governments over these firm's activities is sought by consumers to supervise their actions and ensure users' privacy. Finally, consumers' response in survey shows their expectation from government for imposition of strict laws in the country to maintain data security and transparency in usage of consumer's private data from businesses to ensure information privacy, rightful disclosure of movements of data.

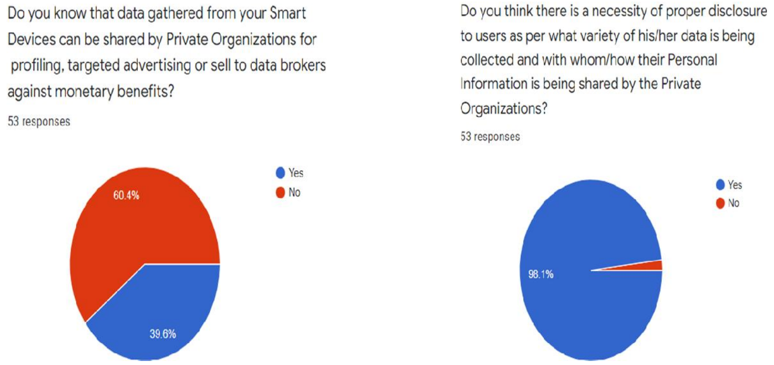

Fig. 4 User's response over awareness and concern about their personal data

VI. Conclusion

This paper uncovers privacy and security risks associated with IoT devices while evaluating user's perception by analysing their responses to the survey. Based on the survey analysis, it can be concluded that most consumers remain unaware of the threats and consequences to their personal data that exists through these gadgets. Further, pursuant to survey results, the paper suggests that laws and regulation in favour of consumers are needed for preserving the confidentiality of users' personal information on all levels of data movement. As the Internet of Things has reached all corners of the globe and with the emergence of Industry 4., privacy concerns will increasingly come to the forefront of discussion. Data breaches, identity thefts and malware have become increasingly common, and it is important that institutions take up necessary actions and regulations to ensure security of data and avoid unfavourable consequences.

REFERENCES

[1]. Alan F. Westin, Privacy and Freedom (New York: Atheneum, 1967).

[2]. Lauren Steinfeld and Kathleen Sutherland Archuleta, "Privacy Protection and Compliance in Higher Education: The Role of the CPO," EDUCAUSE Review, vol. 41, no. 5 (September/October 2006), pp. 62–71.

[3]. Daniel J. Solove A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477 (2006).

[4]. Rehman, Aqeel-ur & Rehman, Sadiq Ur & Khan, Iqbal & Moiz, Malaika & Hasan, S.. (2016). Security and privacy issues in IoT. 8. 147-157.

[5]. 2020 Unit 42 IoT Threat Report," Palo Alto Networks, March 10, 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020.

[6]. M. M. H. ONIK, C. -S. KIM and J. YANG, "Personal Data Privacy Challenges of the Fourth Industrial Revolution," 2019 21st International Conference on Advanced Communication Technology (ICACT), 2019, pp. 635-638, doi: 10.23919/ICACT.2019.8701932.

[7]. G. Culot, F. Fattori, M. Podrecca and M. Sartor, "Addressing Industry 4.0 Cybersecurity Challenges," in IEEE Engineering Management Review, vol. 47, no. 3, pp. 79-86, 1 third quarter, Sept. 2019, doi: 10.1109/EMR.2019.2927559.

[8]. Pereira, Teresa & Barreto, Luis & Amaral, António. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia Manufacturing. 13. 1253-1260. 10.1016/j.promfg.2017.09.047.

[9]. M. Alazab, T. R. Gadekallu and C. Su, "Guest Editorial: Security and Privacy Issues in Industry 4.0 Applications," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6326-6329, Sept. 2022

[10]. Gross, Ralph & Acquisti, Alessandro & III, H.. (2005). Information revelation and privacy in online social networks (The Facebook Case). WPES'05: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society. 71-80. 10.1145/1102199.1102214.

[11]. Kumaraguru, Ponnurangam & Cranor, Lorrie. (2006). Privacy in India: Attitudes and awareness. 243-258.

[12]. Privacy in India: Attitudes and Awareness V 2.0 Ponnurangam Kumaraguru ("PK") Niharika Sachdeva, PreCog-TR-12-001 Nov 22, 2012, Indraprastha Institute of Information Technology, Delhi Okhla New Delhi, 110 020.

[13]. Rosner, Gilad and Rosner, Gilad and Kenneally, Erin E., Privacy and the Internet of Things: Emerging Frameworks for Policy and Design (June 7, 2018).

[14]. Ziegeldorf, Jan & Morchon, Oscar & Wehrle, Klaus. (2014). Privacy in the Internet of Things: Threats and Challenges. Security and Communication Networks. 7. 10.1002/sec.795.

[15]. Pereira, Teresa & Barreto, Luis & Amaral, António. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia Manufacturing. 13. 1253-1260. 10.1016/j.promfg.2017.09.047.

[16]. Mentsiev, Adam & Guzueva, Elina & Magomaev, Tamirlan. (2020). Security challenges of the Industry 4.0. Journal of Physics: Conference Series. 1515. 032074. 10.1088/1742-6596/1515/3/032074.

[17]. G. Culot, F. Fattori, M. Podrecca and M. Sartor, "Addressing Industry 4.0 Cybersecurity Challenges," in IEEE Engineering Management Review, vol. 47, no. 3, pp. 79-86, 1 third quarter, Sept. 2019, doi: 10.1109/EMR.2019.2927559.

[18]. M. M. H. ONIK, C. -S. KIM and J. YANG, "Personal Data Privacy Challenges of the Fourth Industrial Revolution," 2019 21st International Conference on Advanced Communication Technology (ICACT), 2019, pp. 635-638, doi: 10.23919/ICACT.2019.8701932.