Journal for Re Attach Therapy and Developmental Diversities
eISSN: 2589-7799
2023 February; 6 (2s): 145-149

Social and psychological Security of Employee in Association of Internet of things (IoT) and its Privacy and Security Challenges

Ashish Gupta[1], Dr. Susheel Yadav[2], Mr. Ankit Kumar[3]

1Department of Electronics & Communication Engineering, Shivalik College of Engineering, Dehradun
2Shivalik Institute of Professional Studies, Dehradun
3College of Pharmacy, Shivalik, Dehradun
Ashish.gupta@sce.org.in

Received: 28-November-2022
Revised: 07-January-2023
Accepted: 11-February-2023

ABSTRACT: The Internet of Things (IoT) is the worldwide interconnection and use of electronic devices both real and imagined. A special identifier is assigned to each thing. The Internet of Things is a cutting-edge innovation that will revolutionize the way people use electronic gadgets in their daily lives. There are several obstacles that the Internet of Things must overcome, such as incorrect device updates, insufficiently strong security mechanisms, user ignorance, and the ubiquitous but infamous active device monitoring. According to this study, identification, authentication, and also the diversity of IoT devices pose the greatest threats to data security and individual privacy. Integration, scalability, ethical communication mechanism, commercial models, and monitoring are all significant difficulties. The primary concerns of IoT security and privacy are examined in this research. The possibilities of the Internet of Things are infinite. Increasing system flexibility, incorporating artificial intelligence (AI), and the ability to deploy, automate, coordinate, and protect various use cases at hyper-scale would expedite the growth of the manufacturing internet.

Keywords: Electronic devices, Internet of Things (IoT), Radio Frequency Identification (RFID, Security.

1. INTRODUCTION

The Internet of Things (IoT) is a phrase that relates to all linked things and gadgets that are wired or wirelessly linked to the Web. The Internet of Things, or IoT, has grown in popularity as these innovations are employed for a variety of applications, like communications, transport, educational, and commercial growth. IoT introduced the idea of hyper-connectivity which implies that businesses and people may easily interact with one another from the faraway area. The phrase "Internet of Things" was coined by Kevin Ashton in 1999 to popularize the idea of Radio Frequency Identification (RFID), which makes use of integrated sensors and devices. Though the concept itself didn't appear until the 1960s, it has been around for a long time. Pervasive computing or embedded Web were the terms used to describe the concept at the time. Ashton proposed the Internet of Things (IoT) to enhance supply chain operations. Furthermore, IoT's many useful features contributed to the technology's meteoric rise in the summer of 2010. In China, the government has initiated a five-year strategy to make the Internet of Things a top priority. There are now over 26.66 billion connected devices in use [1].

Everything, digital or real, is communicative, addressable, and available over the Internet of Things. Every item would have its unique ID and would be able to perceive, calculate, and interact. Because of the pervasiveness of IoT gadgets, data gathered and transferred for both public and personal use is critical, and data security must be assured. The integrity and privacy of sent data, together with the identification of objects, are critical features of IoT privacy and protection. Users can now track the condition of their security system from their smartphones, start their cars using a mobile app, and operate their garage doors anywhere around the globe. These systems are gradually being integrated into what is being called the "Internet of Things" (IoT). The Internet of Things (IoT) is, at its most fundamental level, the networked interconnection of often disparate devices (such as televisions, utilities, and exercise equipment). Infrastructure, humans, animals, and wildlife can all be monitored in real-time, and a plethora of data may be collected [2].

Many Internet of Things (IoT)-based companies rely on the gathering, analysis, and use of personal data, which may be used to contact or identify an individual, to conduct their operations. Due to the difficulty in forecasting IoT development and the wide discrepancy in forecasts, concrete data should be viewed with some care. Despite this consensus, the fast development of products and services now available on the market lends credence to the idea that the IoT industry will see substantial expansion in the coming years. According to data compiled by IoT Analytics, a specialized market research firm, the number of devices connected in use around the globe in 2018 surpassed 17 billion [3].

Now are other technologies out there that let people manage their dwellings and workplaces with the flick of a wrist. For instance, the Reemo wristbands let you manage your home's entertainment (such as your phone, game console, stereo, and television), safety (such as your alarm and surveillance system), comfort (such as your temperature controller, fire pit, smart fans, and in-floor heating), or utility (such as your outlets, swaps, and dimmable bulbs) with simple arm gestures. Real-time surveillance of property and the actions of individuals in homes and businesses is made feasible by the prevalence of such gadgets. Cybersecurity threats and the ability of rogue apps to access confidential material in IoT systems have risen due to careless usage, failing to change passwords, and failing to update devices. The likelihood of a data breach or other security incident is amplified when such measures are taken. Most security experts agree that IoT is particularly susceptible to cyber assaults because of its lack of robust security measures. Many safeguards have been implemented to prevent hacking of Internet of Things devices, however, there is a lack of documentation on security best practices [4].

2. DISCUSSION

Many established companies are shifting their focus from serving the masses to catering to individual customers, and many more are starting with this strategy as their foundation. Personalizing retail experiences, optimizing journeys, improving health, assisting with financial management, and minimizing energy usage are just some of the many uses for the vast amounts of personal information consumed and produced by the Internet of Things (IoT)-connected devices, such as incredibly advanced smartphones, fitness trackers, household appliances, smart boarding pass gates at train airport terminals, car telematics systems, ‘smart' energy meters, and even linked garments [5]. Radio Frequency Identification, sometimes referred to as RFID, is one of the foundational technologies of the Internet of Things (IoT). Other foundational technologies include Near Field Communication (also known as NFC) and Wireless Sensor Networks (also referred to as WSN).

- *Radio Frequency Identification (RFID*):

The term "Radio Frequency Identification" (RFID) refers to a system that operates wirelessly and is made up of two parts called "readers" and "tags." The reader is a piece of hardware that may include one or more antennas that both send out and receive radio waves to communicate with RFID tags. Tags, which make use of radio waves to convey their identification as well as other data to neighboring readers, may either be active or passive. Active tags transmit their data directly to the reader. There is no need for a battery in passive RFID tags because they get their energy from the reader instead. Batteries are used to power RFID tags that are active. In the IoT, everything has a unique identity and a smart tag attached to it, allowing computers to track it and manage it. Internet of Things devices is equipped with a microcontroller or smart chip which allows them to collect data from their surroundings, analyze that data, and then share their findings with other devices or people. RFID's operational technology and conceptual framework are described in depth. The flaws in the designs of ultra-lightweight authentication mechanisms, as well as the suggested attacks against them and the safety promises they make, have been explored [6].

- *Wireless Sensor Networks (WSN):*

Now more than ever, wireless sensor networks (WSNs) are attracting the interest of scientists and policymakers alike. In a broad sense, a WSN is a network of very tiny nodes that can detect, monitor, collect, analyze, and regulate conditions like data and signals in the local vicinity of an application, facilitating interactions between humans and machines. This makes these nodes very sensitive to factors like battery management, storage, multiplying, data/signal size, or network throughput. These nodes are often static in a predetermined fashion and left as a lone nodes in a distant and uninhabited area to enable tracking and gathering of data [7]. Wireless sensor networks (WSNs) are often used in situations calling for distant sensing applications and data collection. These networks are efficient, productive, and economical [concerning resources]. RFID and WSN have several commonalities in their design and function. However, WSN has the upper hand because of its processing power and intelligence. Potential weaknesses of WSNs and how they should be fixed are discussed in detail. In addition, a consistent algorithm is presented to employ WSNs to address the coverage issue for well-known locations [8].

- *Near Field Communication (NFC):*

This is the backbone technology of the Internet of Things, and it was developed because of the necessity for short-range communications that consume little energy and transfer only small amounts of data. In the context of the internet of things, these technologies enable a wide variety of services, like card readers, transportation, password protection, etc. When two NFC-enabled devices are placed within two centimeters of one other, they

can share data or power using a low-power wireless communication technique called near-field communication (NFC). NFC chips, often known as tags, do not need to be connected to the web to function.

To sum up, the author can state that multiple communications techniques are employed based on the application and its variables such as distance, information, safety, energy consumption, and battery capacity required. The most current technologies for the Internet of Things include Wi-Fi using the IEEE 802.11 ah standard and LoRa using the IEEE 802.15g standard. They're useful since they have a decent data transfer rate and a rather large range [9].

Industrial applications and other commercial uses for IoT-enabled devices are now commonplace. These applications provide these companies an advantage over their rivals. Despite this widespread use, however, the protection and data breach has become a serious worry to most firms since it disrupts the flow of work, operations, and communications networks. To combat these security threats and create comprehensive safety procedures and policies to safeguard company resources and guarantee the reliability of services, experts are required. Smart kitchen house IoT-enabled devices linked to the local area network, for instance, may be a cause of the intrusion for attackers to acquire access to commercial and/or individually sensitive information or to influence and stop the business process.

As IoT encompasses such a wide variety of technologies, it is unrealistic to think of a single IoT design as the de facto reference architecture for all IoT tasks. Since there is no universally accepted design for the Internet of Things, it is quite likely that many reference designs will need to be combined to produce the final design. The optimal IoT design will allow for simple implementation and make the technology's use more appealing to end users [10]. New technologies appear daily, while established ones undergo constant evolution. Think about how far the 5G network has come recently. It is anticipated that 5G would play a pivotal role in IoT infrastructure and software. Its frequency spectrum and bandwidth have piqued the interest of academics concerned about security and privacy. However, because of the short wavelength's insistence on a different infrastructure, more base stations are required to cover the same ground as other wireless technologies. The increased vulnerability to forgery introduced by the new architecture, such as phony base stations, is a major drawback. Knowing the threats and possible countermeasures in terms of security is crucial.

The present state of IoT security has been the subject of several research and services [11]. Many different services have contributed to the problems that various Internet of Things gadgets and associated defenses have had to face. The availability of multiple platforms that could validate these security procedures, as well as a wide range of simulation software and designers, may all contribute to the development of a revolutionary IoT security protocol. Progress in the study of Internet of Things (IoT) safety has been swift, thanks in large part to the different simulation software and designers that have facilitated this study. The consequences would be disastrous if the Internet of Things devices collapsed.

2.1. Potential Threats to Personal Information from the Internet of Things:

Users reaped several advantages from IoT, but it also presented certain difficulties. Researchers and security experts are most concerned with cyber security and privacy threats. This duo is creating a serious problem for many private and governmental institutions. The weaknesses of IoT systems have been exposed by frequent high-profile cyber assaults. This is a problem since the interconnected nature of IoT networks makes them susceptible to attacks from the unidentified and untrustworthy portions of the Internet, necessitating new approaches to safety[12]. Security and privacy concerns are among the most serious obstacles to the widespread use of the Internet of Things. Therefore, it's disappointing that customers typically lack the necessary recognition of the security consequences until after a compromise has happened, resulting in enormous losses like the loss of important data. Users' privacy has been repeatedly breached due to persistent security vulnerabilities, and as a result, customer tolerance for shaky security has decreased. Recent research on the privacy and security of Internet of Things designed for consumers did not provide positive results.

2.1.1. Security:

The IoT's diversity in comparison to conventional computers increases its susceptibility to a wide variety of security threats. IoT adoption has posed new obstacles, despite the fact that the lack of safety in the IT industry is not new. As Internet of Things (IoT) gadgets and services become increasingly pervasive in people's daily lives, it is imperative that users have complete faith in their safety. Among the most important ways in which cyber-attacks may occur and user information could be exposed is via insufficiently secured Internet of Things (IoT) devices and applications. Due to the inherent interconnectedness of IoT devices, a poorly protected or connected item may have far-reaching consequences for the security and reliability of the Internet as a whole. This is a

natural consequence of the difficulty introduced by the widespread adoption of identical IoT devices. Some gadgets have the capacity to dynamically link with others, and this implies that IoT developers and users alike have a responsibility to take precautions against endangering other users and also the Internet as a whole. IoT participants are using a collaborative approach to getting viable answers to the problems they face [13].

2.1.2. Privacy:

When it comes to people's trust in the IoT, the extent to which it can respect their privacy preferences is a key factor in determining that trust's validity. The complete acceptance of IoT may be slowed by worries about privacy and the possible hazards associated with it. Knowing that consumers' privacy rights would be respected is crucial to maintaining their trust in the Internet of Things, the connected device, as well as any associated services. Concerns about privacy have arisen because to the pervasive nature of intelligence-integrated artefacts, which allow for data sampling and dissemination in the IoT to be carried out almost everywhere. The Internet's accessibility from everywhere is a key component in comprehending the issue at hand, as the ease with which private data may be accessed from anywhere in the globe without special measures being taken is a major contributing element to the issue's pervasiveness [14].

2.1.3. Interoperability:

It is well established that a fragmented ecosystem with private IoT technology implementation limits user value. Even though complete interoperability between goods and services is occasionally possible, consumers may dislike purchasing a product or service when there is little flexibility and worries about dealer lock-in poorly conceived IoT devices may have a detrimental impact on the connectivity resources to which they connect.

3. CONCLUSION

Many more novel solutions are undoubtedly required to allow the long-term objective. There is minimal unanimity in the science establishment concerning the architectural and technological solutions to employ for all of the nascent concepts. However, there is a widespread belief that standardisation will be a significant enabler. As a result, IoT security architecture should follow this trend in order to provide an open, ubiquitous, and interoperable infrastructure that is also safe. Smart technologies ought to be able to apply particular, user-defined regulations for the purpose of security and versatility. Infrastructure spy agencies must also be visible and available independent of the link utilised by nomadic smart things.

REFERENCES:

[1] E. Leloglu, “A Review of Security Concerns in Internet of Things,” *J. Comput. Commun.*, vol. 05, no. 01, pp. 121–136, 2017, doi: 10.4236/jcc.2017.51010.

[2] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[3] N. Pepperell and D. Law, “The Internet Imaginary: Between Technology and Technique,” *M/C J.*, vol. 18, no. 2, Apr. 2015, doi: 10.5204/mcj.957.

[4] V. Rozsa, M. L. Dutra, A. L. Pinto, and E. Muriel-Torrado, “Internet of things from information science viewpoint,” *Inf. e Soc.*, 2017.

[5] C. Perera, C. H. Liu, and S. Jayawardena, “The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey,” *IEEE Trans. Emerg. Top. Comput.*, vol. 3, no. 4, pp. 585–598, Dec. 2015, doi: 10.1109/TETC.2015.2390034.

[6] G. Avoine, X. Carpent, and J. Hernandez-Castro, “Pitfalls in Ultralightweight Authentication Protocol Designs,” *IEEE Trans. Mob. Comput.*, vol. 15, no. 9, pp. 2317–2332, Sep. 2016, doi: 10.1109/TMC.2015.2492553.

[7] C. Buratti, A. Conti, D. Dardari, and R. Verdone, “An Overview on Wireless Sensor Networks Technology and Evolution,” *Sensors*, vol. 9, no. 9, pp. 6869–6896, Aug. 2009, doi: 10.3390/s90906869.

[8] Yang Zhang, N. Meratnia, and P. Havinga, “Outlier Detection Techniques for Wireless Sensor Networks: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 12, no. 2, pp. 159–170, 2010, doi: 10.1109/SURV.2010.021510.00088.

[9] W. Sun, M. Choi, and S. Choi, “IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz,” *J. ICT Stand.*, pp. 83–108, Jul. 2013, doi: 10.13052/jicts2245-800X.125.

[10] M. Stočes, J. Vaněk, J. Masner, and J. Pavlík, “Internet of Things (IoT) in Agriculture - Selected Aspects,” *Agris on-line Pap. Econ. Informatics*, vol. VIII, no. 1, pp. 83–88, Mar. 2016, doi: 10.7160/aol.2016.080108.

[11] S. Siby, R. R. Maiti, and N. O. Tippenhauer, "IoTScanner," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, Apr. 2017, pp. 23–30. doi: 10.1145/3055245.3055253.
[12] L. A. Tawalbeh and H. Tawalbeh, "Lightweight Crypto and Security," in *Security and Privacy in Cyber-Physical Systems*, Chichester, UK: John Wiley & Sons, Ltd, 2017, pp. 243–261. doi: 10.1002/9781119226079.ch12.
[13] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017, doi: 10.1016/j.jnca.2017.04.002.
[14] L. A. Tawalbeh and T. F. Somani, "More secure Internet of Things using robust encryption algorithms against side channel attacks," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Nov. 2016, pp. 1–6. doi: 10.1109/AICCSA.2016.7945813.
[15] Panwar, K, Murthy, D, S, "Analysis of thermal characteristics of the ball packed thermal regenerator", *Procedia Engineering*, 127, 1118-1125.
[16] Panwar, K, Murthy, D, S, "*Design and evaluation of pebble bed regenerator with small particles" Materials Today, Proceeding,* 3(10), 3784-3791.
[17] Bisht, N, Gope, P, C, Panwar, K, " *Influence of crack offset distance on the interaction of multiple cracks on the same side in a rectangular plate*", Frattura ed Integrità Strutturale" 9 (32), 1-12.
[18] Panwar, K, Kesarwani, A, "Unsteady CFD Analysis of Regenerator", I*nternational Journal of Scientific & Engineering Research,* 7(12), 277-280.
[19] Singh, I., Bajpai, P. K., & Panwar, K. "*Advances in Materials Engineering and Manufacturing Processes*