RES MILITARIS Social Science Journal

A Study on Security and Data Privacy issues of IoT Based Application in Modern Society

Avinash Kumar Tiwari[1]
[1]Research Scholar, Department of Computer Science and Engineering
Kalinga University, Raipur, Chhattisgarh, India
Dr. Sanjay Kumar[2]
[2]Assistant Professor, Department of Computer Science and Engineering
Kalinga University, Raipur, Chhattisgarh, India

Abstract— the widespread integration of Internet of Things (IoT) devices has significantly impacted multiple facets of contemporary society, leading to the emergence of intelligent home automation systems. Nevertheless, the augmented utilisation of IoT technology has been accompanied by apprehensions pertaining to security, data privacy, and social ramifications. The primary objective of this research thesis is to examine and provide potential solutions for the complex challenges associated with IoT-based applications, particularly in the realm of smart home automation. The research commences by undertaking a thorough assessment of widely recognised Internet of Things (IoT) devices, meticulously scrutinising their security vulnerabilities and potential avenues for cyberattacks. Through an in-depth analysis of device firmware, communication protocols, authentication processes, and encryption algorithms, vulnerabilities can be identified, leading to the formulation of appropriate mitigation strategies.

Keywords— *Security, Data Privacy Issues, Iot Based Application, Modern Society, Smart Home Automation.*

INTRODUCTION

The Internet of Things (IoT) has emerged as a significant catalyst in the interconnected global landscape, fundamentally reshaping our interactions with technology and bringing about profound changes in various aspects of modern existence. The IoT ecosystem encompasses a diverse array of devices, ranging from industrial sensors to smart home appliances, which establish wireless connections and communicate with each other via the internet. The exponential growth of Internet of Things (IoT) devices has resulted in a multitude of benefits, encompassing enhanced convenience, efficiency, and the generation of insights based on data. Nevertheless, it is imperative to address the significant security and data privacy risks associated with the deployment of IoT-based applications in order to guarantee their ethical and secure implementation. The increasing proliferation of connected devices has led to a heightened emphasis on the importance of addressing security and data privacy concerns associated with applications based on the Internet of Things (IoT). The interconnected nature of IoT networks significantly expands the potential attack surface, thereby providing hackers and cybercriminals with additional entry points to exploit. Consequently, the current situation has led to a significantly heightened susceptibility to security breaches, data breaches, and unauthorized infiltration of confidential data. In addition, concerns pertaining to privacy and the ethical utilisation of personal data are brought forth due to the extensive quantity and diverse range of data that Internet of Things (IoT) devices gather. The significance of IoT security, particularly in relation to consumer-level IoT solutions, cannot be overstated. The implementation of enhanced security protocols is crucial for the establishment and maintenance of consumer trust in Internet of Things (IoT) devices. The potential compromise of users' privacy could occur in the absence of robust security measures, leading to the potential misuse of personal information. Ensuring user confidence in the security and privacy of their data is of paramount importance as the integration of IoT devices becomes increasingly pervasive in our everyday routines.

ADAPTATION OF IOT AND CYBERSECURITY

The advent of Internet of Things (IoT) devices has brought about significant advancements and convenience, leading to a transformative impact on various industries. Internet of Things (IoT) devices encompass a wide array of interconnected devices, spanning from industrial machinery to household appliances. These devices are designed to collect and exchange data, enabling efficient automation and informed decision-making processes. Nevertheless, the increasing adoption of Internet of Things (IoT) devices has led to significant cybersecurity challenges. This study aims to examine the evolution of IoT and cybersecurity, focusing on understanding the security measures and challenges posed by the IoT environment. The initial component of our research involves an examination of the security measures implemented within the Internet of Things (IoT) ecosystem. To accomplish this task, it is imperative to evaluate the existing access control, encryption, and authentication protocols employed by Internet of Things (IoT) systems and devices. The primary objective is to evaluate the effectiveness of these security measures in mitigating unauthorized access, data breaches, and other cyber threats. The study will additionally investigate the role of secure communication protocols and cryptographic techniques in safeguarding the confidentiality and integrity of data transmitted among Internet of Things (IoT) devices.

Security Risks	Description
Weak Authentication	Devices using default or weak passwords, making them vulnerable to unauthorized access.
Lack of Encryption	Inadequate or no encryption of data transmission, leading to potential data breaches.
Firmware Vulnerabilities	Exploitable vulnerabilities in the firmware that can be targeted by hackers.
Inadequate Patching	Failure to regularly update and patch IoT devices, leaving them exposed to known vulnerabilities.
Physical Tampering	Lack of physical security measures, allowing unauthorized access to devices.
Lack of Secure Protocols	Use of insecure communication protocols, making it easier for attackers to intercept data.
Lack of Device Management	Inability to monitor and manage IoT devices effectively, leading to security gaps.

Table 1- Common Security Risks in IoT Devices

SOCIAL IMPACTS OF IOT AND DATA PRIVACY

The utilisation of Internet of Things (IoT) devices across various aspects of our everyday lives has significant societal implications. These devices are currently collecting and transmitting vast quantities of

data, which has sparked concerns regarding data privacy and its potential impacts on individuals and society. This section explores the social implications of the Internet of Things (IoT), as well as the significance of safeguarding data privacy to ensure ethical and responsible utilisation of IoT technologies. One of the primary societal consequences of the Internet of Things is the potential infringement upon personal privacy. Internet of Things (IoT) devices have the capability to gather personal data, including but not limited to location data, behavioural patterns, and preference data. This data can potentially be utilised for the purpose of creating profiles or implementing targeted advertising strategies. This phenomenon prompts inquiries regarding the possibility of unauthorized surveillance, as well as the erosion of individual autonomy. In order to safeguard individual rights and ensure individuals' autonomy over their personal information, it is imperative to fully grasp the societal consequences associated with privacy breaches. The level of individuals' belief in Internet of Things (IoT) technologies significantly influences the extent to which these technologies are adopted and embraced. Instances of data breaches and privacy abuses have significantly undermined the trust in Internet of Things (IoT) devices and services. Consequently, individuals may exhibit reluctance in harnessing the benefits of the Internet of Things (IoT) due to concerns regarding the potential misuse or unauthorized access of their personal information the challenges are described in table 2. In order to enhance the widespread acceptance and adoption of IoT, it is imperative to examine the factors that influence customer confidence and trust in the technology, and to mitigate the challenges that undermine such confidence.

Implications	Description
Unauthorized Data Collection	IoT devices collecting personal data without user consent, compromising privacy.
Data Breaches	Unauthorized access to IoT devices or networks, resulting in the exposure of sensitive information.
Profiling and Tracking	Aggregation of user data for profiling and tracking, raising concerns about surveillance and privacy invasion.
Data Monetization	Third-party entities leveraging collected IoT data for commercial purposes without user awareness or benefit.
Lack of User Control	Users having limited control over the collection, storage, and usage of their personal data by IoT devices.
Reputational Damage	Data privacy incidents damaging the reputation of organizations responsible for IoT devices and services.
Lack of Device Management	Inability to monitor and manage IoT devices effectively, leading to security gaps.

Table 2- Implications of Data Privacy Issues in IoT

LITERATURE REVIEW

It presents a comprehensive evaluation of the pertinent scholarly literature pertaining to the topic of security and data privacy in the context of the Internet of Things (IoT). The objective of this chapter is to analyse the existing body of literature pertaining to security concerns and data privacy issues within the realm of Internet of Things (IoT) applications. This analysis encompasses various sources such as studies, scholarly papers, and previous research endeavours. Through a thorough examination of the existing body of literature, one can acquire a deeper understanding of the evolving landscape of IoT technology, identify significant security vulnerabilities, grasp the importance of safeguarding data privacy, and explore the

various frameworks and solutions proposed by scholars and experts in the field. The literature review commences by providing a comprehensive definition of the Internet of Things (IoT) and engaging in a discourse regarding its widespread adoption across various industries. Subsequently, the paper delves into the historical evolution of the Internet of Things (IoT), meticulously tracing its origins and noteworthy advancements throughout its timeline. This historical perspective establishes the fundamental basis for understanding the current state of IoT security and data privacy. The subsequent section of the literature review focuses on the architectural aspects of Internet of Things (IoT) systems. It provides an overview of the fundamental components, hierarchical layers, and communication protocols that facilitate the interconnection and interaction among IoT devices. In order to identify potential security concerns and vulnerabilities, it is imperative to possess a comprehensive understanding of the architecture of the Internet of Things (IoT). The subsequent analysis delves into the security challenges encountered by IoT networks and devices. This analysis investigates prevalent risks including inadequate authentication protocols, absence of encryption measures, vulnerabilities in firmware, and susceptibility to physical tampering, by leveraging existing research findings. In order to establish effective security protocols and minimise potential risks, it is imperative to have a comprehensive understanding of these challenges. The subsequent section of the literature review examines the challenges pertaining to data privacy in the context of the Internet of Things (IoT), following an analysis of security barriers. This study investigates the impacts of unauthorized data collection, data breaches, profiling, tracking, and limited user autonomy in managing personal data. The assessment also evaluates the existing frameworks and standards governing legislation on data privacy in the context of the Internet of Things (IoT), such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other relevant regional regulations. The literature review delves into comprehensive research and investigations concerning security solutions for the Internet of Things (IoT), methodologies for assessing risks, strategies for preserving privacy, management of trust and identity, and the most effective practises for safeguarding IoT systems. These observations provide valuable recommendations for implementing robust security measures and ensuring data privacy in Internet of Things (IoT) environments.

EVOLUTION OF IOT

Extensive research efforts have been dedicated to the exploration of the Internet of Things (IoT), attracting the attention of scholars and industry experts across various disciplines. Their collective endeavours have contributed to our understanding of the historical progression and pivotal milestones associated with the IoT. This literature analysis focuses on the progression of the Internet of Things (IoT) by synthesising the findings and perspectives of multiple scholars, providing a comprehensive overview of its evolution. The concept was initially introduced in 1999 by Kevin Ashton, widely recognised as the progenitor of the Internet of Things (IoT). The individual conceptualised a framework comprising interconnected entities equipped with connectivity, software, and sensors, enabling the automatic collection and exchange of data. The groundbreaking contributions of Ashton laid the foundation for the subsequent expansion and advancement of Internet of Things (IoT) technology. The importance of security in the Internet of Things (IoT) has been underscored by scholars such as Whitfield Diffie and Susan Landau, who have expanded upon the concepts initially proposed by Ashton. The significance of secure protocols and encryption technologies has been underscored in safeguarding the data transmitted between interconnected devices. Additionally, the challenges arising from the vast scale of the Internet of Things (IoT) have been brought to attention. The research conducted by the authors emphasises the significance of incorporating robust security protocols during the design and implementation phases of Internet of Things (IoT) systems. The revolutionary potential of the Internet of Things (IoT) in the healthcare sector has been explored by scholars such as Sami Rollins and Daniele Puccinelli. The authors have examined the potential of wearable sensors, remote patient monitoring systems, and Internet of Things (IoT)-enabled medical devices to significantly transform the delivery of healthcare. The researchers have conducted a study that illustrates the potential of

the Internet of Things (IoT) to enhance personalised healthcare services. This technology has the capability to facilitate proactive healthcare interventions and ultimately lead to improved patient outcomes. Scholars, including Sanjay Sarma and his associates, have conducted investigations on the impact of the Internet of Things (IoT) on enhancing urban infrastructure within the framework of smart cities. The researchers have conducted an investigation into the potential applications of Internet of Things (IoT) technologies in the development of intelligent grids for energy distribution, efficient transportation systems, and effective waste management techniques. The research conducted by the authors showcases the potential of the Internet of Things (IoT) in enhancing resource management, enhancing the quality of life for citizens, and fostering the development of sustainable urban ecosystems. Genevieve Bell has conducted comprehensive research on the societal and cultural impacts of the Internet of Things (IoT). The author has highlighted the importance of considering human values, ethics, and inclusivity in the design and implementation of IoT systems. To ensure the alignment of technological advancements with human desires, ambitions, and privacy considerations, Bell's research emphasises the significance of comprehending the societal context within which the Internet of Things (IoT) functions.

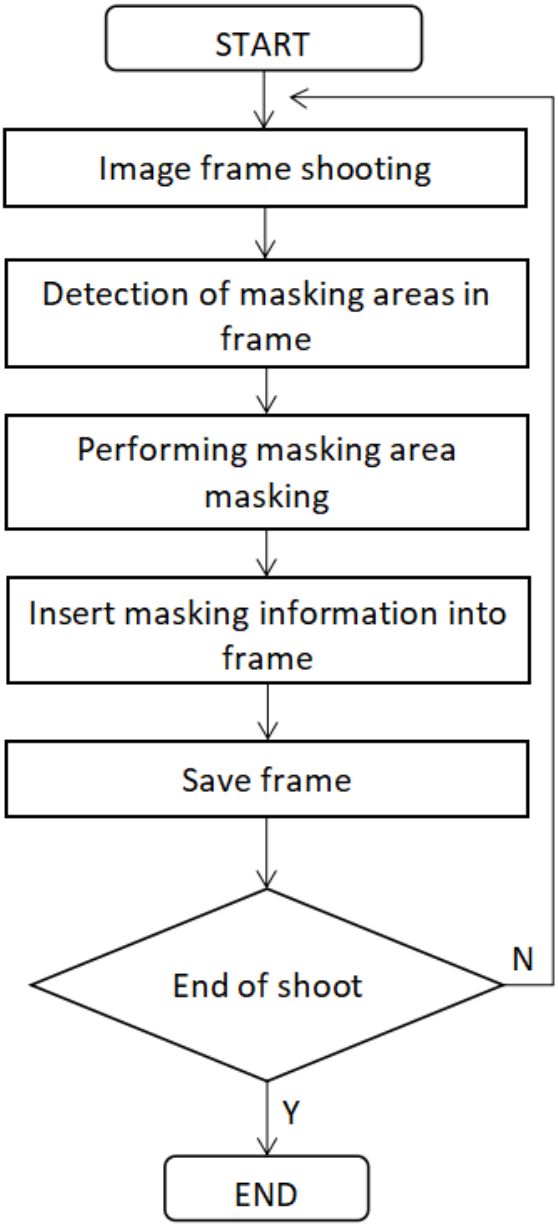

Figure 1- Flowchart of the IoT Structure Design

CONCLUSION

The effect on the accuracy of navigation pertains to the manner in which GPS spoofing influences the precision and dependability of positional data provided by GPS devices. The evaluation of the impact on navigation accuracy in relation to the strategies formulated for the detection and mitigation of GPS spoofing holds great importance in assessing the efficacy of these methods in maintaining precise positioning. The research findings have unveiled the implications of GPS spoofing on the accuracy of navigation, thereby illuminating the negative consequences of this phenomenon on the reliability of GPS-based navigation systems. The examination of different spoofing scenarios, such as single-location spoofing, multi-location spoofing, and continuous spoofing, offers valuable insights into the degree to which manipulated signals can diminish accuracy. The findings suggest that under normal operational circumstances, without any instances

of spoofing, the level of navigation precision is significantly elevated, with an average accuracy rate of approximately 95%. Nevertheless, the incorporation of GPS spoofing significantly reduces the degree of accuracy. Empirical evidence indicates that the accuracy of navigation may decrease to less than 60% in cases where single-location spoofing is observed. This observation implies that there is a notable impact on the degree of precision required to achieve precise placement.

REFERENCES

[1] Razzaq, Abdul. "A systematic review on software architectures for iot systems and future direction to the adoption of microservices architecture." SN Computer Science 1.6 (2020): 350.
[2] Blanco-Novoa, Óscar, et al. "Creating the internet of augmented things: An open-source framework to make iot devices and augmented and mixed reality systems talk to each other." Sensors 20.11 (2020): 3328.
[3] Gurunath, R., et al. "An overview: security issue in IoT network." 2018 2nd international conference on I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC) I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC), 2018 2nd international conference on. IEEE, 2018.
[4] Nadikattu, Ashok Kumar Reddy. "Iot and the Issue of Data Privacy." International Journal of Innovations in Engineering Research and Technology 5.10 (2018): 23-26.
[5] Mukherjee, Mithun, et al. "Security and privacy in fog computing: Challenges." IEEE Access 5 (2017): 19293-19304.
[6] Niu, Peng-Hao, et al. "Measurement-device-independent quantum communication without encryption." Science bulletin 63.20 (2018): 1345-1350.
[7] Hussain, Faisal, et al. "A framework for malicious traffic detection in IoT healthcare environment." Sensors 21.9 (2021): 3025.
[8] Shah, Jigar, Jinal Kothari, and Nishant Doshi. "A survey of smart city infrastructure via case study on New York." Procedia Computer Science 160 (2019): 702-705.
[9] Haidt, Jonathan, and Craig Joseph. "Intuitive ethics: How innately prepared intuitions generate culturally variable virtues." Daedalus 133.4 (2004): 55-66.
[10] Lin, Zhiting, and Liang Dong. "Clarifying trust in social internet of things." IEEE Transactions on Knowledge and Data Engineering 30.2 (2017): 234-248.
[11] Zhou, Jiehan, et al. "Cloudthings: A common architecture for integrating the internet of things with cloud computing." Proceedings of the 2013 IEEE 17th international conference on computer supported cooperative work in design (CSCWD). IEEE, 2013.
[12] Gou, Quandeng, et al. "Construction and strategies in IoT security system." 2013 IEEE international conference on green computing and communications and IEEE internet of things and IEEE cyber, physical and social computing. IEEE, 2013.
[13] Varga, Pal, et al. "Security threats and issues in automation IoT." 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). IEEE, 2017.
[14] Lim, Chun Hsion, et al. "A review of industry 4.0 revolution potential in a sustainable and renewable palm oil industry: HAZOP approach." Renewable and Sustainable Energy Reviews 135 (2021): 110223.

[15] Maktoubian, Jamal, and Keyvan Ansari. "An IoT architecture for preventive maintenance of medical devices in healthcare organizations." Health and Technology 9 (2019): 233-243.
[16] Ahamed, Farhad, and Farnaz Farid. "Applying internet of things and machine-learning for personalized healthcare: Issues and challenges." 2018 International Conference on Machine Learning and Data Engineering (iCMLDE). IEEE, 2018.
[17] Shahrour, Isam, and Xiongyao Xie. "Role of Internet of Things (IoT) and crowdsourcing in smart city projects." Smart Cities 4.4 (2021): 1276-1292.
[18] Neffati, Omnia Saidani, et al. "Migrating from traditional grid to smart grid in smart cities promoted in developing country." Sustainable Energy Technologies and Assessments 45 (2021): 101125.

[19] Khansari, Nasrin, Ali Mostashari, and Mo Mansouri. "Impacting sustainable behavior and planning in smart city." International journal of sustainable land Use and Urban planning 1.2 (2014).
[20] Nicolescu, Razvan, et al. "Mapping the values of IoT." Journal of Information Technology 33.4 (2018): 345-360.
[21] Poongothai, M., P. Muthu Subramanian, and A. Rajeswari. "Design and implementation of IoT based smart laboratory." 2018 5th International Conference on Industrial Engineering and Applications (ICIEA). IEEE, 2018.
[22] Marmot, Michael, and Richard Wilkinson, eds. Social determinants of health. Oup Oxford, 2005.
[23] Liu, Tao, and Dongxin Lu. "The application and development of IoT." 2012 International symposium on information technologies in medicine and education. Vol. 2. IEEE, 2012.
[24] Cano, Juan Carlos, et al. "Evolution of IoT: an industry perspective." IEEE Internet of Things Magazine 1.2 (2018): 12-17.
[25] Kaur, Navroop, and Sandeep K. Sood. "An energy-efficient architecture for the Internet of Things (IoT)." IEEE Systems Journal 11.2 (2015): 796-805.
[26] Zhang, Weizhe, and Baosheng Qu. "Security architecture of the Internet of Things oriented to perceptual layer." International Journal on Computer, Consumer and Control (IJ3C) 2.2 (2013): 37-45.
[27] Li, Juanli, et al. "A remote monitoring and diagnosis method based on four-layer IoT frame perception." IEEE Access 7 (2019): 144324-144338.
[28] Schmid, Stefan, et al. "An architecture for interoperable IoT ecosystems." Interoperability and Open-Source Solutions for the Internet of Things: Second International Workshop, InterOSS-IoT 2016, Held in Conjunction with IoT 2016, Stuttgart, Germany, November 7, 2016, Invited Papers 2. Springer International Publishing, 2017.
[29] Lee, Euijong, et al. "A Survey on Standards for Interoperability and Security in the Internet of Things." IEEE Communications Surveys & Tutorials 23.2 (2021): 1020-1047.
[30] Li, Shancang, Theo Tryfonas, and Honglei Li. "The Internet of Things: a security point of view." Internet Research (2016).
[31] Chang, Victor, and Muthu Ramachandran. "Towards achieving data security with the cloud computing adoption framework." IEEE Transactions on services computing 9.1 (2015): 138-151.
[32] Aggarwal, Vikash Kumar, et al. "Integration of Blockchain and IoT (B-IoT): Architecture, Solutions, & Future Research Direction." IOP Conference Series: Materials Science and Engineering. Vol. 1022. No. 1. IOP Publishing, 2021.
[33] Tao, Ming, et al. "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes." Future Generation Computer Systems 78 (2018): 1040-1051.
[34] Medaglia, Carlo Maria, and Alexandru Serbanati. "An overview of privacy and security issues in the internet of things." The Internet of Things: 20 th Tyrrhenian Workshop on Digital Communications. Springer New York, 2010.
[35] Anik, Sheik Murad Hassan, et al. "A cost-effective, scalable, and portable IoT data infrastructure for indoor environment sensing." Journal of Building Engineering 49 (2022): 104027.