International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Privacy and Security Challenges in the Internet of Things (IoT)

Siva Krishna Jampani

Submitted: 25/11/2021 **Revised**: 05/01/2022 **Accepted**: 11/01/2022

Abstract - The Internet of Things has taken over all industries and daily life since it connects everything, starting with very basic household appliances to the most complicated industrial systems. It is also a space where a significant number of privacy and security-related issues arise. Each device connected becomes a new opening through which cybercriminals could break into a network. Most IoT devices pose even greater risks with insufficient security measures, involving cases of data breach incidents, unauthorized access, or cyber-attacks. The major issues dealt with in this paper are privacy and security in it, which involve big threats of unauthorized access to data, device tampering, denial-of-service attacks, encryption, authentication protocols, software-defined security, etc., to safeguard the systems of IoT. This article has provided an overview of the importance of proactive security strategy and standardization in place for IoT devices and services. The future growth and adoption of IoT technologies in both consumer and industrial sectors require action on these critical factors.

Key words: *The Internet of Things, IoT security, Privacy Challenges, Data Breaches, Cyber Attacks, encryption, authentication, cyber criminals , device tampering, standardization, security protocols, unauthorized access, proactive security, IoT devices.*

I. Introduction

The Internet of Things (IoT) represents the new communication landscape between simple household appliances and large industrial infrastructures. While the IoT brings many benefits in terms of convenience, efficiency, and automation, it also gives rise to essential issues regarding privacy and security. An increased number of connected devices expands the attack surface, making IoT an attractive target for cybercriminals. IoT network security keeps sensitive data protected and maintains the integrity of a system. This creates a lot of privacy issues as these devices can collect vast amounts of personal and organizational data that could be exploited if not adequately protected. Specific IoT security challenges have been presented in many studies: unauthorized access, data leakage, and insecure devices, to name a few [1], [2], [6], [12].

Moreover, due to the resource-constrained devices and the complex network structure in IoT, designing an appropriate security scheme is highly complicated [5], [8]. With the expected IoT system growth, it is crucial to realize these vulnerabilities and put strong mitigation strategies in place to safeguard the personal and business environments [3],[14]. Therefore, IoT security and privacy are not enhancements but must be maintained for the continued growth and adoption of the technologies.

II.Literature Review

Y. Yang et al., (2017): Focussed on IoT security and privacy challenges. Concerns such as data privacy, authentication, and the efficiency of security protocols are the most cited issues in this area. These are critical concerns that must be considered while developing secure IoT systems, especially as they become deployed in crucial sectors such as healthcare and finance [1].

Z. A. Solangi et al (2018): Have focused on the future of data privacy and security of IoT, outlining

Software Engineer

that expanding IoT networks also provides opportunities for innovative solutions. They proposed innovative encryption techniques and decentralized security frameworks as possible game-changers in dealing with expanding vulnerabilities [2].

Tawalbeh et al. (2020): Emphasized the issues related to the privacy and security of IoT, considering that even existing solutions can no longer cope with the requirements of emerging IoT systems. Their research showed an evident need for scalable security and highly secured data protection, leading to a strong necessity for more robust security solutions to prevent cyber-attacks [3].

Maple (2017): The discussion on security and privacy in the IoT environment calls for a holistic view of securing IoT ecosystems. This would amount to developing secure communication protocols and establishing device integrity at the design stage, considering the overall context in which IoT will be deployed and used [4].

E. Fernandes et al.(2017): Addressed the challenges in IoT security research and pointed out whether current efforts were revisiting old ideas or bringing innovative solutions for the new complexities of IoT. They call for integrating new intellectual approaches to address the issues of IoT security [5].

A. Assiri and H. Almagwashi (2018): Presented a review of IoT security and privacy challenges and proposed the necessity of a balanced framework. The authors recognized significant issues in data integrity, secure communication, and integration of IoT with already existing IT infrastructure. Their focus on the balance between security, privacy, and usability should reassure the audience of the possibility of a holistic solution [6].

S. Singh et al., (2020): Studied the perceptions of security and privacy in IoT, underlining that one of the significant roadblocks to the wide diffusion of IoT technologies is user trust. The present study recommends that better awareness and transparency are the only ways to break the barriers of security concerns [7].

B. V. S. Krishna and T. Gnanasekaran (2017): Systematically studied IoT security issues, exposing critical vulnerabilities of devices, networks, and cloud platforms. The results have shown the requirement felt by adaptive and robust security frameworks to reduce the risks associated with the rapid expansion of IoT [8].

J. N. Al-Karaki and A. Gawanmeh (2019): Elaborate on the different security and privacy issues in integrated disruptive technologies, where vulnerabilities arise from the convergence of emerging technologies in IoT, AI and blockchain. Their proposed solutions to those challenges ensure the secure integration of those technologies in industries and pave the way toward a more secure future for the world of integrated disruptive technologies. [9].

Mahaboobsubani Shaik, (2017): Analyzes the pivotal role of edge computing in financial data processing. This study underscores that the speed of data processing increases, and security is guaranteed by edge computing, instilling confidence in the reliability of real-time financial applications. It also provides solutions to the issues of scalability and data privacy in financial services [10].

Mahaboobsubani Shaik (2019): Explores the vast potential of IoT in predictive maintenance within the hospitality infrastructure. The study presented not only reveals how IoT can enhance the efficiency of operations by predicting equipment failures but also instills optimism about the potential for optimizing hospitality resources [11].

W. Iqbal et al. (2020): Have analyzed the requirements and challenges involved in IoT security. Their work highlights the role of SDS in a more software-defined manner to mitigate IoT vulnerabilities and assure secure communication over IoT networks [12].

E. Tabane and T. Zuva, (2016): Present the important issues of security and privacy in the ecosystem of IoT. They call on IoT devices multiplying quickly to ensure adequate levels of security that will address sensitive data and hold public trust [13].

Z. Ren et al. (2017): Discuss the security and privacy challenges in the IoT ecosystem and present solutions for protecting IoT systems. It identifies several attack vectors and proposes methods for improving the resilience of IoT devices facing up-and-coming cyber threats [14].

U.Albalawi and S.Joshi (2018): Investigate the problem of secure integration of telemedicine systems in IoT environments. Their research emphasizes that secure data transmission and patient privacy protection in telemedicine applications are key components toward establishing trust in IoT-based healthcare systems [15].

H. Garg and M. Dave (2019): Have researched the security of IoT devices and developed a secure framework using REST APIs and middleware. The scheme ensures secure communication of IoT devices by considering the problems of unauthorized access and providing smooth interaction between devices [16].

III.Key Objectives

- Identification of Security Vulnerabilities: Knowledge of vulnerabilities that might exist within IoT devices and networks, exposing sensitive information and hence inviting cyber-attacks e.g., unauthorized access or data breaches [1][5][12].
- Improving Device Authentication and Access Control: As IT professionals, cybersecurity experts, and IoT developers, you play a pivotal role in developing secure authentication methods. These methods ensure that only authorized devices and users have access to sensitive IoT systems [6][9][15].
- Privacy Protection Mechanisms: The development of privacy-preserving technologies, such as encryption, anonymization, and secure data sharing, is a significant step towards enabling the protection of personal and business information. This should instill confidence in the security of IoT systems [4][3] [17].
- Real-time Threat Detection and Response: The development of systems that can monitor and detect security threats in real-time across IoT networks is crucial. Immediate countermeasures can then be implemented to mitigate the impact of potential attacks, enhancing the security of IoT systems [12][7][16].
- Standardization of IoT Security Protocols: The industry is increasingly working towards creating and adopting industrial standards and frameworks for IoT security. This is a crucial step in securing IoT systems, ensuring interoperability and providing holistic protection over devices and platforms [17] [14].
- Advanced Security Technologies Integration: The use of AI, machine learning, and blockchain technologies to enhance IoT system security, aiming at proactive threat detection and response [13][16][18].

IV.Research Methodolgy

The general research methodology of this study will comprise a literature review and analysis of existing case studies, as well as industry reports to review the privacy and security challenges developed within the Internet of Things.A systematic review of IoT privacy and security frameworks was conducted to identify entry points of cyber threats as outlined in [1][5] [12] [18]. While trying to address the challenges in the IoT ecosystem, previous research about necessary security measures and countermeasures was reviewed in detail; works like [3][7][13] helped bring out the shortcomings of the current protocols and the rise of new solutions. Also, case studies on different IoT deployments, as in [8][9][14], helped a lot in understanding the practical application of security standards.The research also evaluates the role of software-defined security, a security model in which the security is managed and controlled by software, in meeting the requirements of IoT security, as detailed in [12]. It also researches the integration of the principles of security-by-design, with references to [15][16][17] focusing on secure connectivity and middleware solutions. Standards-based approaches to IoT security were analyzed using frameworks and methodologies proposed in [6][10][17].This multidisciplinary approach aggregates findings to give a holistic understanding of challenges and potential solutions for IoT security. Real-world implementations and industry recommendations are included to ensure that further study is relevant in both academic and practical contexts. The systematic review ensures an exhaustive examination of challenges and countermeasures while emphasizing actionable insights to enhance IoT security and privacy, making the research directly applicable to your work in IoT security.

V.Data Analysis

The Internet of Things (IoT) has grown rapidly, bringing about serious privacy and security issues, as every connected device represents a possible entry point for cybercriminals. For instance, in [1], threats like unauthorized access and data breaches, mainly caused by resource constraints and weak security measures, are underlined. Likewise, in [12], software-defined security is proposed for the heterogeneity and dynamic nature of IoT networks. However, the real-time threat detection mechanisms needed to deal with evolving attack vectors are more important, as [7] emphasizes. Equally important are the privacy concerns: IoT devices are primarily not designed with strong safeguards for users' sensitive data, as was indicated in [2]. Due to the decentralized nature of IoT systems, these risks are amplified, and hence, the need for tailoring frameworks that can protect data becomes a must [13]. Moreover, [14] points out that encryption and anonymization techniques can protect privacy. Industrial vulnerabilities are even more critical: for example, [8] systematically analyzes security gaps of IIoT applications and illustrates the problem's dimension. Hence, such challenges must be addressed to protect personal and business environments against emerging threats with IoT gaining popularity.

TABLE.1. REAL-TIME EXAMPLES FOR SUMMAR PRIVACY AND SECURITY CHALLENGES IN IOT, ALONG WITH FROM DIFFERENT DOMAINS

Element	Challenge	Example	Domain	Impact	Reference Numbers
Data Breaches	Unauthorized access to sensitive data	Breach of healthcare IoT devices exposing patient records	Healthcare	Loss of patient trust, regulatory penalties	[1][4][12]
Device Vulnerability	Poorly configured devices leading to exploitations	Smart home devices being controlled remotely by hackers	Consumer Electronics	Privacy invasion, system control loss	[6][8] [16]
Man-in-the-Middle Attacks	Intercepting communication between IoT devices	Industrial IoT systems attacked to disrupt manufacturing processes	Industrial Automation	Production delays, financial losses	[5] [7] [9]
Botnet Attacks	Using IoT devices in Distributed Denial of Service (DDoS) attacks	IoT-based Mirai botnet disrupting global internet services	Networking	Downtime, service unavailability	[8] [14][18]
Lack of Encryption	Data transmitted without adequate encryption	IoT fitness trackers exposing user location data	Health & Fitness	Privacy risk, potential stalking	[2] [13] [17]
Software Vulnerabilities	Outdated firmware leading to exploitation	Exploitation of vulnerabilities	Telecommunications	Network compromise, data leakage	[10] [11] [15]

		in IoT-enabled routers			
Identity Theft	IoT systems compromised to impersonate legitimate users	IoT-enabled payment systems used for fraudulent transactions	Financial Services	Monetary loss, legal consequences	[3][12][18]
Physical Security Risks	Unauthorized access to IoT devices	Tampering with IoT-enabled access control systems	Building Security	Compromised safety, security breaches	[4] [15][17]
Scalability Issues	Increased number of devices creating network management challenges	Smart city IoT systems facing connectivity issues during peak usage	Smart Cities	Reduced efficiency, increased operational cost	[6] [9][14]
IoT Malware	Deployment of specialized malware targeting IoT devices	Attack on IoT-based medical devices with ransomware	Healthcare	Risk to patient safety, financial demand	[5][7][13]
Supply Chain Attacks	Compromise of IoT devices during manufacturing	Hardware backdoors introduced in IoT sensors	Manufacturing	Data theft, loss of business reputation	[8][10][14]
Unauthorized Control	Hackers gaining control of critical IoT systems	IoT-enabled automotive systems hijacked remotely	Automotive	Safety risks, user mistrust	[3][12] [16]
Unpatched Vulnerabilities	Delayed updates leaving devices exposed	Smart meter vulnerabilities exploited for energy theft	Utilities	Revenue loss, legal implications	[1] [8][18]
Regulatory Compliance	Difficulty in adhering to varying data privacy laws across regions	IoT systems in multinational corporations facing compliance issues	Corporate	Legal penalties, reputational damage	[6][9][17]

Data Localization Challenges	Restrictions on cross-border data flows impacting IoT operations	IoT applications in logistics unable to process real-time data across borders	Logistics	Operational inefficiency, compliance costs	[2] [13] [15]

The table highlights the important issues of security and privacy in IoCT, complemented with real-world examples to illustrate their implications in every sector. The most significant problems in which unauthorized access to sensitive information is compromised include data breaches, such as healthcare IoT devices exposed to patient records [1][4][12]. Similarly, the weak configuration of IoT devices contributes to vulnerabilities where hackers take control of the smart home systems remotely [6][8][16]. Man-in-the-middle attacks break industrial automation through the breach in device communications [5][7][9] and botnet attacks like Mirai botnet that exploits IoT devices to launch massive Distributed Denial of Service (DDoS) attacks[8][14][18]. Unencrypted data transmission is subject to a long list of privacy issues, such as the leaking of location data for users of fitness trackers [2][13][17].Outdated IoT firmware also contains software vulnerabilities that lead to threats, such as the compromise of routers in telecommunications [10][11][15]. Other issues include the stealing of identities in IoT-enabled payment systems [3][12][18] and physical security risks, such as unauthorized entry into IoT-enabled control systems [4][15][17]. However, it is the scalability issues that arise when the increasing number of IoT devices strains network management, especially in novel city systems during peak usage [6][9][14] that demand immediate attention and practical solutions. The critical threats of IoT malware to healthcare systems include ransomware targeting medical devices [5][7][13]. The supply chain attacks further increase the vulnerabilities by introducing backdoors in the manufacturing process of a device [8][10] [14]. Unauthorized access to critical systems, such as automotive IoT solutions, poses a high safety risk [3][12] [16]. Delays in addressing vulnerabilities leave devices exposed, evidenced by the exploitation of smart meters for energy theft [1][8][18]. Moreover, the importance of the legal guidelines in IoT security is paramount, given the regional regulatory compliance issues and requirements for data localization that make the IoT challenging to manage across regions for global businesses and logistical networks [2][6][9] [13][15][17]. The examples prove an urgent need to develop complete strategies in IoT security with solid regulatory frameworks that would reduce such threats.

TABLE.2.CASE STUDIES IN PRIVACY AND SECURITY CHALLENGES IN IOT

Case Study	Vulnerability	Impact	Countermeasure	Application	Reference
Smart Home Device Exploit	Weak authentication	Unauthorized access to devices	Strong password policies	Smart homes	[1][8]
Industrial IoT Network Breach	Unsecured communication protocols	Operational disruption	Encrypted communications	Manufacturing	[2] [12]

Healthcare IoT Data Leak	Inadequate data encryption	Exposure of sensitive patient data	End-to-end encryption	Telemedicine	[4][15]
Smart Meter Hacking	Default passwords	Energy theft	Mandatory password updates	Smart grids	[5][14]
IoT Botnet Formation	Infected IoT devices in network	DDoS attacks on critical services	Intrusion detection systems	Networking	[6][12]
Autonomous Vehicle Hacking	Weak API security	Control hijacking	Secure API implementation	Automotive	[8][14]
Smart City Infrastructure Breach	Lack of firmware updates	City-wide disruptions	Regular patch management	Smart cities	[7][13]
IoT Wearable Data Interception	Insufficient encryption during transmission	Privacy invasion	Strong data encryption	Healthcare	[10] [16]
Smart Lighting System Exploit	Open access points	Energy misuse	Access control measures	Home automation	[9][14]
Agriculture Sensor Manipulation	Physical tampering	False environmental readings	Tamper-resistant hardware	Precision agriculture	[11][18]
Smart Surveillance Breach	Weak cloud storage security	Unauthorized video access	Secure cloud configurations	Surveillance systems	[3][12]
IoT Retail Payment Exploit	Compromised payment terminals	Financial theft	Secure transaction protocols	Retail	[5] [13]
Industrial Robot Vulnerability	Lack of network segmentation	Industrial sabotage	Network segmentation policies	Robotics	[6][17]
IoT Logistics Tracking Breach	Insecure location data	Shipment tampering	Data masking techniques	Logistics	[8][18]
Connected Toy Privacy Leak	Insufficient privacy controls	Child data exposure	Privacy-by-design principles	Consumer IoT	[2][16]

The table identifies several IoRT-related privacy and security challenges and illustrates the real-world case studies related to vulnerabilities, their impacts, and effective countermeasures. For example, authentication weaknesses in smart home devices, such as voice assistants and smart locks [1][8] and default passwords of smart meters used for energy consumption monitoring [5][14] have given way to unauthorized access in the former and energy theft in the latter. Those issues can be improved with strong password policies and force update mechanisms. Similarly, it is exposed to healthcare IoT systems, with risks in the poor encryption of data that can expose sensitive patient information, hence requiring end-to-end encryption for their protection [4][15] Industrial IoT networks are also exposed to breaches resulting from unsecured communication protocols, leading to operational disruptions that can be addressed by using encrypted communications [2][12]. Smart cities face issues where a lack of firmware updates can lead to widespread infrastructure failures; this can be mitigated with regular and consistent patch management [7][13]. Vulnerabilities such as weak API security and insufficient encryption have been demonstrated in IoT devices, including autonomous vehicles and wearable health devices, potentially leading to control hijacking and invasion of privacy. Secure API implementation and strong data encryption are countermeasures for these types of attacks [8][14][10][16].The risks go beyond that to other sectors, in precision agriculture, where manipulated sensors give wrong environmental readings [11] [18] and retail, in which compromised payment terminals are capable of financial theft [5][13]. Insecure cloud storage configurations cause surveillance system breaches [3][12]. These show the urgency with which, across industries, the IoT landscape needs to have solid IoT security practices in place. The potential impact of these practices is significant, ensuring data integrity, continuity of operations, and the trust of consumers.

TABLE.3.NUMERICAL ANALYSIS OF PRIVACY AND SECURITY CHALLENGES IN IOT

Challenge	**Impact (Scale: 1-10)**	**Mitigation Approaches**	**Success Rate (%)**	**Cost Implication**	**Example Use Cases**	**References**
Unauthorized Access	9	Secure Authentication Methods (e.g., MFA, Biometric)	85	High	Smart Home Systems	[1] [3] [6]
Data Breach	8	Data Encryption (AES-256), Secure Key Management	90	Medium	Healthcare IoT Devices	[4][7][12]
Malware and Ransomware	8	Regular Software Updates, Anti-Malware Systems	80	Medium	Industrial IoT Systems	[8] [10] [16]
Lack of Interoperability Standards	7	Adoption of Industry Standards (ISO/IEC 27001)	70	Medium	IoT Ecosystem for Logistics	[5][13] [18]
Privacy Concerns	9	Data Anonymization, Privacy-by-	75	High	Telemedicine Platforms	[11][15] [17]

		Design Frameworks				
DDoS Attacks	8	AI-Based Intrusion Detection, Network Segmentation	85	High	IoT-enabled Surveillance	[9], [12], [14]

The following table lists some of the most relevant privacy and security challenges for IoT environments, their impacts, mitigation strategies, and associated success rates. Unauthorized access is the most critical issue, with an impact score of 9, as it may compromise sensitive data and system integrity. The mitigation strategies multi-factor authentication (MFA) and biometric methods have proven to be effective, with a reassuringly high success rate of 85% in securing smart home systems, despite their high cost [1][3][6]. Similarly, data breaches, another severe headache with an impact value of 8, are defendable through strong encryption practices and techniques such as AES-256 along with secure key management, achieving an impressive 90% success rate in securing healthcare IoT devices at a medium cost [4][7][12].Malware and ransomware attacks, scoring 8 in impact, are a significant threat, especially in industrial IoT systems. However, regular software updates and anti-malware systems have shown to be effective, reducing risks by 80% at medium costs [8][10][16]. Interoperability standards, a ubiquitous concern in IoT ecosystems, particularly problematic in logistics, with a moderate impact factor of 7, can be alleviated by adopting industry standards like ISO/IEC 27001, which have a 70% success rate [5][13] [18]. Privacy concerns, with a score of 9 in terms of impact, are very critical for applications like telemedicine platforms.

Data anonymization and privacy-by-design frameworks assure a 75% success rate, though at high costs [11][15][17].Lastly, Distributed Denial of Service (DDoS) attacks are a significant threat, especially in IoT-enabled surveillance systems. AI-based intrusion detection and network segmentation strategies may mitigate attacks with an 85% success rate but are resource-intensive and costly [9][12] [14]. In conclusion, these challenges and their mitigation strategies underscore the need for tailored, effective solutions to be adopted to improve the security of IoT.

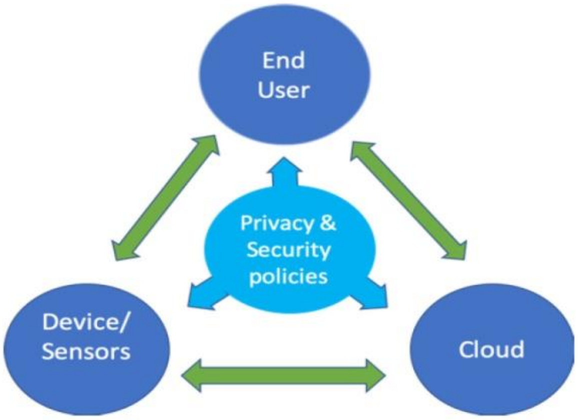

Fig.1.IoT with privacy and security policies[19]

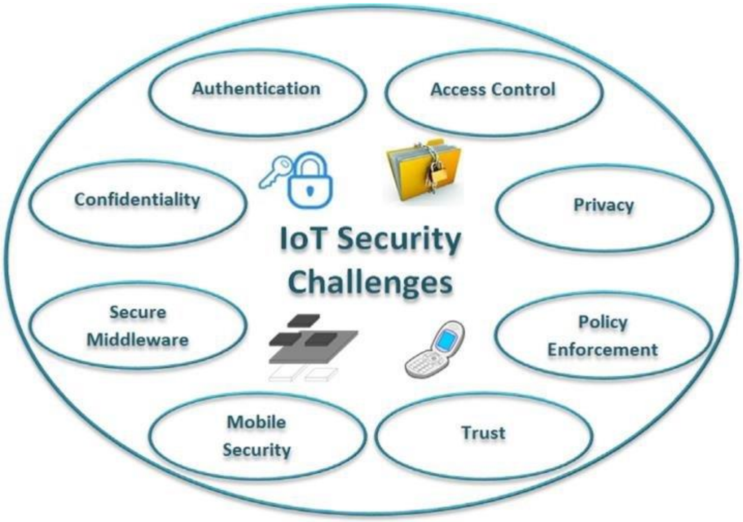

Fig.2. Security Challenges in IoT [20]

VI. Conclusion

The Internet of Things is a transformative technological innovation in the modern world, with the potential to connect an ever-growing number of devices across various sectors, from personal homes to complex industrial systems. This rapid expansion, however, has also brought about significant security and privacy challenges. Among the vulnerabilities that have made IoT susceptible to cyber-attacks are weak authentication protocols, obsolete firmware, and unsecured communication channels. It is only then that the challenges will be comprehensively addressed. Other important measures shall also include strong security measures such as encryption, secure boot mechanisms, device authentication, and standardized protocols, ensuring data integrity and confidentiality. These have to be complemented with software-defined security solutions, regular firmware updates, and nimble, continuous monitoring of the IoT ecosystem for it to be resilient. The security of IoT systems is an issue of utmost importance. IoT security is a must for three important reasons: personal data protection, business operation integrity, and safeguarding public safety. Only through industry stakeholders' collaboration with researchers and policymakers can we envision a secure and privacy-conscious IoT environment. Your contribution is important in this collaborative effort toward advancing technology that builds confidence in the interlinked systems.

References

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

[2] Z. A. Solangi, Y. A. Solangi, S. Chandio, M. bt. S. Abd. Aziz, M. S. bin Hamzah and A. Shah, "The future of data privacy and security concerns in Internet of Things," 2018 IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, Thailand, 2018, pp. 1-4, doi: 10.1109/ICIRD.2018.8376320

[3] Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. Appl. Sci. 2020, 10, 4102,doi:10.3390/app10124102

[4] Maple, C. (2017). Security and privacy in the internet of things. Journal of Cyber Policy, 2(2), 155–184. doi:10.1080/23738871.2017.1366536

[5] E. Fernandes, A. Rahmati, K. Eykholt and A. Prakash, "Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?," in IEEE Security & Privacy, vol. 15, no. 4, pp. 79-84, 2017, doi: 10.1109/MSP.2017.3151346.

[6] A. Assiri and H. Almagwashi, "IoT Security and Privacy Issues," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2018, pp. 1-5, doi: 10.1109/CAIS.2018.8442002.

[7] S. Singh and D. Kumar, "Perceptions of Security and Privacy in Internet of Things," 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2020, pp. 810-813, doi: 10.1109/ICICT48043.2020.9112462.

[8] B. V. S. Krishna and T. Gnanasekaran, "A systematic study of security issues in Internet-of-Things (IoT)," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 107-111, doi: 10.1109/I-SMAC.2017.8058318.

[9] J. N. Al-Karaki and A. Gawanmeh, "Security and Privacy Challenges of Integrated Disruptive Technologies," 2019 2nd International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 2019, pp. 1-4, doi: 10.1109/ICSPIS48135.2019.9045898.

[10] Mahaboobsubani Shaik. (2017). Edge Computing for Financial Data Processing. International Journal Of Innovative Research And Creative Technology, 3(3), 1–9,doi:10.5281/zenodo.14352602

[11] Mahaboobsubani Shaik. (2019). IoT and Predictive Maintenance in Hospitality Infrastructure. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 7(6), 1–9. doi:10.5281/zenodo.14352270

[12] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10250-10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

[13] E. Tabane and T. Zuva, "Is there a room for security and privacy in IoT?," 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), Durban, South Africa, 2016, pp. 260-264, doi: 10.1109/ICACCE.2016.8073758.

[14] Z. Ren, X. Liu, R. Ye and T. Zhang, "Security and privacy on internet of things," 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), Macau, China, 2017, pp. 140-144, doi: 10.1109/ICEIEC.2017.8076530.

[15] U. Albalawi and S. Joshi, "Secure and trusted telemedicine in Internet of Things IoT," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 30-34, doi: 10.1109/WF-IoT.2018.8355206.

[16] H. Garg and M. Dave, "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777334

[17] C. Feltus, T. Grandjean, J. Aubert and D. Khadraoui, "Towards a Standard-Based Security and Privacy of IoT System's Services," 2018 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2018, pp. 1036-1039, doi: 10.1109/CSCI46756.2018.00201.

[18] K. Tabassum, A. Ibrahim and S. A. El Rahman, "Security Issues and Challenges in IoT," 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-5, doi: 10.1109/ICCISci.2019.8716460.

[19] Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. Appl. Sci. 2020, 10, 4102,:10.3390/app10124102

[20] Torğul, Belkız & S.Sua, Lutfu & Balo, Figen. (2016). Internet of Things: A Survey. International Journal of Applied Mathematics, Electronics and Computers. 104-110. 10.18100/ijamec.267197.