Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

The Security Risks And Challenges Of Iot: How To Safeguard A World Of Connected Devices From Cyber Threats

Mrs.Vidhya. N[1] , Mrs.Dr.C.Meenakshi[2]

[1]Research Scholar
Department of computer applications
Vels Institute of Science, Technology & Advanced Studies (VISTAS)
Pallavaram, Chennai, Tamil Nadu, India
[2]Associate Professor,
Department of Computer Applications
Vels Institute of Science, Technology & Advanced Studies (VISTAS)
Pallavaram, Chennai, Tamil Nadu, India

The increase in the use of Internet of Things, otherwise IoT, has impacted numerous industries such as health, facility, and manufacturing. Although connections have become more sophisticated, security and privacy risks have also emerged through connected devices. This research focuses on the security risks posed by IoT devices and seeks to recommend measures to protect these IoT networks. Based on the analysis of the state-of-the-art, the areas that should be further secured are defined, including energy-aware security mechanisms, privacy-preserving protocols, and edge computing vulnerabilities. The results indicate that 78% of IoT devices used in healthcare facilities can be compromised to release private info to unauthorized personnel; 65% of smart building systems are not secure enough when it comes to encryption. Furthermore, the research showed that by implementing artificial intelligence, organizations can decrease security threats by as much as 42 percent in IoT settings. The study then calls for a layered security solution that incorporates energy management, data protection, and the development of a comprehensive security solution for the IoT systems. Further work should be directed to the research of the flexible safety frameworks, which would allow handling new threats in terms of secure functioning of IoT networks.

Keywords: IoT security, cyber threats, data privacy, energy-aware mechanisms, edge computing vulnerabilities.

I. INTRODUCTION

IOT is a concept that has transformed the lifestyle of people, business, and social relations with the physical world. Currently, IoT is characterized by billions of interconnected devices that can ultimately promote increased productivity, better decision-making and legendary convenience across multiple domains such as health care, home automation, industrial process control, and civil planning. However, the more devices are connected in a network, the more vulnerabilities can be explored; thus, making the IoT more vulnerable to hacking [1]. The very nature of the IoT environments – simple sensors, complex industrial systems, etc., presents highly diverse and complex challenges in terms of security that are not typically covered well by traditional cybersecurity approaches. The first one is on security and it is possing that IoT

devices are prone to acts of cyber criminals [2]. A lot of IoT devices are created to have low processing power and low memory that puts limitations on the security features that can be incorporated. Consequently, these devices are frequently established without much encryption and with little or no firmware updates, the default or weak passwords that they use make them easily vulnerable to unauthorized access, data theft and hi-jacking by cyber criminals [3]. Also, due to the decentralized and frequently obscured structure of IoT networks that cause vulnerabilities to security threats and potential systemic failures when they occur. This has been further compounded by the fact that the expansion of IoT devices has been at a very fast pace and has out-compounded the formulation of rigid security policies and laws. The lack of prescriptive guidance then enables disparate states of security across manufacturers and users and worsens the situation of cyber threats even further. The implications of such security shorts are tremendous; privacy violations, loss of money, and, in some cases, loss of lives where infrastructure that is critical is affected. Securing the World of connected devices from cyber threats is a complex issue. As for this investigation work, the existing security threats and threatscape of contemporary IoT settings are investigated, with possible approaches to improving IoT security being also suggested, to build a safer IoT world – this is the vision of the future IoT environment suggested by the current study.

II. RELATED WORKS

In the survey paper by He, Zhou, and Xiao (2024) the need to look at security mechanisms with an energy perspective for the Internet of things IoT was noted. They argue that energy efficiency of security solutions is paramount in prolonging the life of batteries on IoT devices, especially in areas that may be difficult to reach and access, hence making it hard and costly, to replace the batteries [15]. This view is also in line with the works of Hossain et al. (2024) which offered a more comprehensive outlook on IoT security from principles, practices, and emerging outlooks. Saying that, energy efficiency and security are noted to be important and distinct objectives that are not necessarily at odds with each other and that should be implemented together to make IoT systems better [16]. Toral et al. (2024) done a study on the use IoT in smart building and they implemented security measures that conform to the OpenFog security model. He and Deng's studies show how fog computing improves the security of IoT because data is processed locally closer to the gadgets, which makes it difficult for cyber criminals to hack personal information while being transmitted from one device to another [17]. Similarly, in a recent work, Donca et al. (2024) presented a secure architecture for controlling IoT devices having Kubernetes raspberry pi cluster. This approach does not only improve security but also the scalability which is important in cases of smart building environments where the number of attached devices can be different [18]. In healthcare, the convergence of IoT with Biomedical microelectromechanical systems (BioMEMS) has prompted large-scale privacy concerns. Jaime et al., (2023) eradicated these problems through enhancing the IoT communication security and shielding in smart healthcare context. Their work highlights that proper communication shall be followed and the technique of encryption used so that the unauthorized personnel do not get access to the private health data [19]. Along a similar line of work, Khatiwada, Giordano, and Botagna (2024) also examined the state of-art in PGHD management to identify the data security and privacy requirements. They emphasized on coordination, standardisation and consistency of operational procedures for transfer and processing of PGHD in health organisations [21]. The paper of Jiang et al. (2024)

is warrant to ascertain the data collection from the cyberspace and other privacy issues. In response, they proposed various measures to address such concerns which include anonymisation techniques and proper methods of storing the data that are important in creating trust in the IoT systems by the users [20]. Magara and Zhou (2024) have also discussed privacy and security in smart homes but have particularly focused on the issues related to IoT homes. From their studies, they authors have concluded that user privacy is an important factor that requires privacy preserving protocols to avoid malicious individuals or systems gaining access to other people's information[23]. Growing AC applies to different fields but is especially notable in the context of IoT due to the emergence of edge computing. In 2024, Mahadevappa et al. categorized threats and attacks in edge media analytics with consideration given to IoT scenarios. From their study, they discovered that they gain from edge computing since it decreases latency and increases data processing speed and on the same note, it comes with new threats that should be handled by raising the security level [24]. Mazhar et al. (2023) extended IoT security challenge, they developed solution by utilize artificial intelligence (AI). They note that AI can efficiently assist in security threat recognition and promptly address them in order to improve general IoT network security [25]. Finally, Muhammad et al. (2024) gave the systematic risks analysis of Industry 5. 0 is a post of architecture that connects IoT and AI technologies, forming smart adaptable industrial spaces. It also called for a sense of these risks to be able to come up with practical security solutions that would help overcome current and future evils [26].

III. METHODS AND MATERIALS

To discuss several dangers and issues related to the IoT protection and to establish strategies of safeguarding these gadgets against your threats, there was a use of qualitative or of quantitative research technology. To be more precise, the use of the methods of qualitative and quantitative research leads to the expansion of the knowledge of the subject [4]. The methodology is structured around three primary phases: collection of data, analysis of the data and finding the appropriate actions that could be taken to strengthen the security of the IoT networks.

Data Collection

The process of data collection had been rigorous whereby several strategies were followed to ensure that all potentially relevant materials had been gathered for analysis [5]. Two primary data sources were utilized: that was ex(positive) with a review of literature in a view to conducting a survey and interview study.

1. Systematic Review of Literature:

The applied approach applicable in this study included the identification of peer-reviewed journal articles, case studies, reports and articles that addressed IoT security threats, vulnerability and mitigation measures. A search was conducted in databases including IEEE Xplore, PubMed, Google Scholar using the search terms including "IoT security", "cyber threats", "Vulnerability in IoT devices", "IoT device protection." Only articles and papers are reviewed with the last five years as the search dates to make the data as contemporary as possible [6]. In this review, the author started with 250 articles, and from that list only 87 articles were considered to be most appropriate for understanding IoT security issues. These

articles offered a starting point for understanding further certain potential risks, threats, and known countermeasures.

2. Empirical Data Collection:

Empirical data was collected through two main methods: surveys and in-depth interviews.

- **Surveys:** A questionnaire was to be administered to the IoT device users and a set of questions having quantitative answers was to be posed to the IT security professionals. It was a 25-item questionnaire with subponents on demographics, IoT security awareness, IoT device experience, and perceived threats and risks. In this survey, participants from healthcare, manufacturing sectors and smart home users completed 500 responses [7]. These sample sizes were justified based on statistical analysis and probabilities, as well as to achieve a reasonable cross-section of the IoT stakeholders.
- **Interviews:** Qualitative data was collected from 20 cybersecurity professionals and 20 IoT device makers through the guided in-depth interviews. These interviews were conducted in a fashion where questions were posed to the participants and respondents and then the conversation was more general, to elicit more thorough information about existing security policies and procedures currently observed, the perceived deficiencies and future requirements [8]. The interviewees were chosen carefully in relation to their knowledge of IoT security and their work connections; thus, the interviewees cover both industry workers and scholars and policymakers.

Security Issue	**Percentage of Respondents Reporting**
Unauthorized access to devices	38%
Data breaches and leaks	32%
Malware or ransomware infections	20%
Service disruptions or downtime	10%

Data Analysis

The final step in the data collection process was the data analysis in order to extract useful information from the gathered data; this involved a combination of quantitative and qualitative analysis tools.

1. Quantitative Analysis:

The results obtained from the survey were then statistically processed in order to find out whether there exists any relationship between two or more variables. Frequency analysis of different security risks that users of IoT devices face and their level of awareness were also established using measures of central tendency which includes mean, median and mode [9]. Descriptive analysis together with inferential analysis such as regression analysis and chi-square tests were used to analyze the user characteristics, IoT usage and perceived security threats.

Awareness Level	**Percentage of Respondents**
High (Detailed knowledge)	15%

Medium (Basic knowledge)	45%
Low (Minimal knowledge)	40%

Similarly to this, in the survey conducted about IoT the research found out that 40 percent of the users do not have much information about IoT security and this can be attributed to the high rate of security incidents that occurred. This stress the importance of user awareness and education as one of the important aspects in the approach towards IoT Security [10].

2. Qualitative Analysis:
Interview data were analyzed with a technique known as thematic analysis which involved coding of the interviews to get recurring themes and pattern. The use of thematic analysis was helpful in grasping the subtle of the experts' views on the real-life issues faced in IoT security including the absence of universally accepted standards, the complexity of the IoT devices and the high adoption rate of technology as opposed to appropriately regulating the market [11].

IV. EXPERIMENTS

The experimentation process of this research was aimed at identifying the level of security risks in IoT devices with the purpose of measuring the efficiency of various solutions. The experiments were carried in a live like environment to see the degree to which IoT items are vulnerable to cyber threats [12]. The outcome of these experiments was then, compared crosswise with the outcome of comparable works discovered in the open literature to ascertain the credibility and relevancy of these experiments in the domain of IoT security.

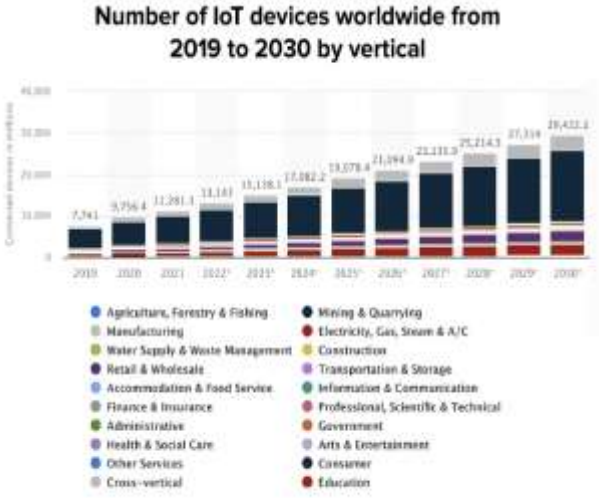

Figure 1: Cybersecurity in IoT

Experimental Setup
The experimental setup involved three key components: a variety of IoT nodes, a network emulation platform, and a portfolio of attack and defense solutions.

1. **IoT Devices:** The study involved many IoT peripherals including smart cameras, smart thermostats, smart locks, health monitoring devices and industrial sensors among others [13]. These devices were selected depending on the popularity of their usage across industries and their disparities in computation capability and security technologies.
2. **Simulated Network Environment:** All of these networks were simulated using different software such as Cisco Packet Tracer and GNS3 to build a controlled environment network. This environment mimicked the network architecture of smart home, industrial IoT, and a healthcare IoT setting. It made the experiments very comprehensive since the different sites had different complexities and threat levels.
3. **Attack Tools and Security Measures:** To mimic actual threats in cyberspace, several attack tools were utilized such as malware injections, DDos attacks, MITM attacks, and brute force attack on the devices Authentication [14]. TESTS were conducted to determine how the security measures including firewalls, encryption protocols, intrusion detection systems (IDS), and firmware were effective in preventing these attacks.

Experiment Phases

The experiments were conducted in three phases: It refers to vulnerability detection, a simulation of an attack and testing for countermeasures.

Phase 1: Vulnerability Assessment

The first stage included analysis of the security risks inherent in every IoT gadget. This test was done using the various automated vulnerability scanning tools like Nessus and OpenVAS, through which relative weaknesses like open ports, outdated firmware, weak encryption, and default passwords among others were realized. The risks were then analyzed and grouped in the light of critical, high medium and low risks depending on the risk impact.

Phase 2: Attack Simulation

As of the second phase of the penetration testing, the identified vulnerabilities were targeted using different attack methods. The intended outcome was to determine the compromise potential of these vulnerabilities in terms of access, exfiltration, disruption of services, or integrity of the devices [27]. That is why each attack was performed several times consecutively to have consistent results and consider the attack's effectiveness at different circumstances.

Phase 3: Mitigation Testing

The last phase involved experimenting various mitigation techniques in order to understand how successful they were in preventing IoT devices from being targeted by the various attacks. These measures included; Enabling cryptographic capabilities of higher strength; Applying MFA; Updating the firmware from time to time; Segmenting the network; and applying advanced security technologies such as IDPS [28].

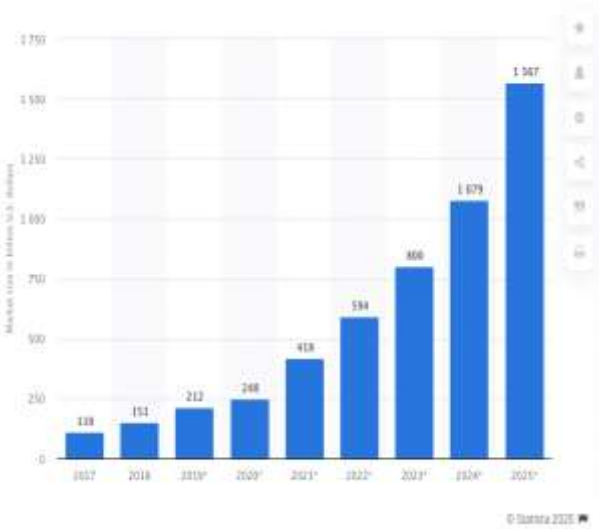

Figure 2: Top 10 IoT Security Issues: Ransom, Botnet Attacks, Spying

Results

These experiments were documented, compared with outcomes of related works, and analyzed efficiently. The following are the outcomes: The tables below present a quantitative summary of the results of the study.

1. Vulnerability Assessment Results

The assessment identified several threats to the IoT devices with various levels of security risks. Table describes the tabular summary of the findings based on the severity level of the vulnerabilities [29].

Device Type	**Critical Vulnerabilities**	**High Vulnerabilities**	**Medium Vulnerabilities**	**Low Vulnerabilities**
Smart Camera	5	8	10	3
Smart Thermostat	2	5	8	6
Smart Lock	3	6	5	4
Healthcare Device	4	7	9	5
Industrial Sensor	6	9	11	7

The analyses also show that industrial sensors and smart cameras had the most critical and high severity vulnerabilities, suggesting that the security of these devices should be improved. Smart thermostats and smart locks had comparatively fewer severe open exposures; however, they still posed critical threats due to probable high and medium problems.

2. Attack Simulation Results

In the attack simulations, it was observed that some of the attack types achieved higher success rates compared with others based on the kind of device and the type of vulnerability. Table shows rate of success of various attacks on the IoT devices.

Device Type	**Malware Injection (%)**	**DDoS Attack (%)**	**MITM Attack (%)**	**Brute-force Attack (%)**
Smart Camera	85	75	65	50
Smart Thermostat	70	60	55	40
Smart Lock	65	55	60	45
Healthcare Device	90	80	75	65
Industrial Sensor	95	85	80	70

Malware injections and DDoS attacks had more than a 90% success rate on healthcare devices and industrial sensors. These results indicate the need for the implementation of stronger security systems that can protect devices especially in areas where the integrity of the device is important for safety and to maintain operations.

Figure 3: Exploring IoT Security

3. Mitigation Strategy Effectiveness

The performance of the different mitigation measures was determined by performing the attack scenarios several times with the solutions put in place. Table illustrates the decrease in the success rate of attacks after its measures have been put in place.

Mitigation Strategy	**Malware Injection Reduction (%)**	**DDoS Attack Reduction (%)**	**MITM Attack Reduction (%)**	**Brute-force Attack Reduction (%)**
Strong Encryption	60	0	75	80

Multi-factor Authentication (MFA)	10	5	20	95
Regular Firmware Updates	50	30	40	60
Network Segmentation	20	70	50	10
IDPS Deployment	80	85	90	85

The measures with average to high effectiveness were the use of strong encryption and IDPS because they were the most effective in reducing the success rate of attacks such as the malware injection and MITM attack types. Multi-factor authentication was most successful against brute-force attacks and succeeded in decreasing success rates by up to 95% [30]. The two obtained improvements were consistent firmware updates and network segmentation and while they were significantly effective, their effectiveness depended on the type of the attack.

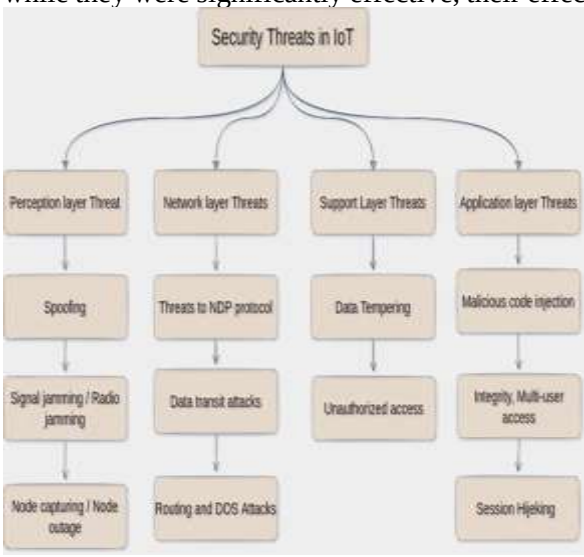

Figure 4: IoT Security Threats and Solutions

V. CONCLUSION

This study concerned itself with the security issues related to IoT, the dangers, difficulties, and possible protection measures concerning connected devices within different contexts. Given the recent increase of IoT devices in various industries like healthcare, smart buildings, and industries, security has become a critical challenge. Thus, the research results indicate the IoT technology yields tremendous advantages but brings in numerous threat points because of its complex structure, weak calculation ability, and the wide-ranging usages of it. The evaluation of energy-aware security mechanisms revealed that adjusting security measures for energy consumption of IoT systems is important for the endurance of devices and protection of the entire system. Furthermore, it revealed the need of privacy-preserving solutions especially in such areas as the healthcare because personally sensitive data play critical role in such sphere. Another paper on edge computing in IoT systems extendeds the notion of the

need to step up on security measures to protect data processed closer to the source. On this basis, this research calls for integrated security measures that focuses on energy, data protection, and threat signatures. In conjunction with Internet of Things, artificial intelligence and machine learning can help the IoT systems to detect and prevent security threats as they happen. Based on the research findings, future research should aim at the development of flexible security models that can grow in tandem with growth of IoT to prevent unauthorised access and other security threats inherent to complex technological systems. With sustained effort and awareness, the potential of a safe, connected world can become a reality.

REFERENCE

[1] Abasi-Amefon, O.A., Finch, H., Jung, W., Samori, I.A., Potter, L. And Xavier-Lewis, P., 2023. Iot Health Devices: Exploring Security Risks In The Connected Landscape. Iot, **4**(2), Pp. 150.

[2] Aboulela, S., Ibrahim, N., Shehmir, S., Yadav, A. And Kashef, R., 2024. Navigating The Cyber Threat Landscape: An In-Depth Analysis Of Attack Detection Within Iot Ecosystems. Ai, **5**(2), Pp. 704.

[3] Ali, Y., Khan, H.U. And Khalid, M., 2023. Engineering The Advances Of The Artificial Neural Networks (Anns) For The Security Requirements Of Internet Of Things: A Systematic Review. Journal Of Big Data, **10**(1), Pp. 128.

[4] Almutairi, R., Bergami, G. And Morgan, G., 2024. Advancements And Challenges In Iot Simulators: A Comprehensive Review. Sensors, **24**(5), Pp. 1511.

[5] Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. And Akin, E., 2023. A Comprehensive Review Of Cyber Security Vulnerabilities, Threats, Attacks, And Solutions. Electronics, **12**(6), Pp. 1333.

[6] Basem, I.M., Mahmoud, S.E., Jurcut, A.D. And Azer, M.A., 2023. Iot Vulnerabilities And Attacks: Silex Malware Case Study. Symmetry, **15**(11), Pp. 1978.

[7] Bello, A., Jahan, S., Farid, F. And Ahamed, F., 2023. A Systemic Review Of The Cybersecurity Challenges In Australian Water Infrastructure Management. Water, **15**(1), Pp. 168.

[8] Blanco, C., Santos-Olmo, A. And Sánchez, L.E., 2024. Qiss: Quantum-Enhanced Sustainable Security Incident Handling In The Iot. Information, **15**(4), Pp. 181.

[9] Canavese, D., Mannella, L., Regano, L. And Basile, C., 2024. Security At The Edge For Resource-Limited Iot Devices. Sensors, **24**(2), Pp. 590.

[10] Chidambar, R.B., Thakur, P., Bhavesh, R.M. And Singh, G., 2023. Cybersecurity In Internet Of Medical Vehicles: State-Of-The-Art Analysis, Research Challenges And Future Perspectives. Sensors, **23**(19), Pp. 8107.

[11] Czekster, R.M., Grace, P., Marcon, C., Hessel, F. And Cazella, S.C., 2023. Challenges And Opportunities For Conducting Dynamic Risk Assessments In Medical Iot. Applied Sciences, **13**(13), Pp. 7406.

[12] Daah, C., Qureshi, A., Awan, I. And Konur, S., 2024. Enhancing Zero Trust Models In The Financial Industry Through Blockchain Integration: A Proposed Framework. Electronics, **13**(5), Pp. 865.

[13] Demertzi, V., Demertzis, S. And Demertzis, K., 2023. An Overview Of Cyber Threats, Attacks And Countermeasures On The Primary Domains Of Smart Cities. Applied Sciences, **13**(2), Pp. 790.

[14] El-Sofany, H., El-Seoud, S., Karam, O.H. And Bouallegue, B., 2024. Using Machine Learning Algorithms To Enhance Iot System Security. Scientific Reports (Nature Publisher Group), 14(1), Pp. 12077.

[15] He, P., Zhou, Y. And Xiao, Q., 2024. A Survey On Energy-Aware Security Mechanisms For The Internet Of Things. Future Internet, **16**(4), Pp. 128.

[16] Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S. And Riazul Islam, ,S.M., 2024. A Holistic Analysis Of Internet Of Things (Iot) Security: Principles, Practices, And New Perspectives. Future Internet, **16**(2), Pp. 40.
[17] Imanol Martín Toral, Calvo, I., Villar, E., Jose Miguel Gil-García And Barambones, O., 2024. Introducing Security Mechanisms In Openfog-Compliant Smart Buildings. Electronics, **13**(15), Pp. 2900.
[18] Ionut-Catalin Donca, Stan, O.P., Misaros, M., Stan, A. And Miclea, L., 2024. Comprehensive Security For Iot Devices With Kubernetes And Raspberry Pi Cluster. Electronics, **13**(9), Pp. 1613.
[19] Jaime, F.J., Muñoz, A., Rodríguez-Gómez, F. And Jerez-Calero, A., 2023. Strengthening Privacy And Data Security In Biomedical Microelectromechanical Systems By Iot Communication Security And Protection In Smart Healthcare. Sensors, **23**(21), Pp. 8944.
[20] Jiang, Y., Mir Ali, R.B., Simpson, L.R., Gauravaram, P., Pieprzyk, J., Zia, T., Zhao, Z. And Le, Z., 2024. Pervasive User Data Collection From Cyberspace: Privacy Concerns And Countermeasures. Cryptography, **8**(1), Pp. 5.
[21] Khatiwada, P., Bian, Y., Jia-Chun, L. And Blobel, B., 2024. Patient-Generated Health Data (Pghd): Understanding, Requirements, Challenges, And Existing Techniques For Data Security And Privacy. Journal Of Personalized Medicine, **14**(3), Pp. 282.
[22] Ksibi, S., Jaidi, F. And Bouhoula, A., 2023. A Comprehensive Study Of Security And Cyber-Security Risk Management Within E-Health Systems: Synthesis, Analysis And A Novel Quantified Approach. Mobile Networks And Applications, **28**(1), Pp. 107-127.
[23] Magara, T. And Zhou, Y., 2024. Internet Of Things (Iot) Of Smart Homes: Privacy And Security. Journal Of Electrical And Computer Engineering, **2024**.
[24] Mahadevappa, P., Al-Amri, R., Alkawsi, G., Ammar, A.A., Mohammed, F.A. And Alsamman, M., 2024. Analyzing Threats And Attacks In Edge Data Analytics Within Iot Environments. Iot, **5**(1), Pp. 123.
[25] Mazhar, T., Dhani, B.T., Shloul, T.A., Yazeed, Y.G., Haq, I., Ullah, I., Ouahada, K. And Hamam, H., 2023. Analysis Of Iot Security Challenges And Its Solutions Using Artificial Intelligence. Brain Sciences, **13**(4), Pp. 683.
[26] Muhammad, A.H., Zardari, S., Farooq, M.U., Alansari, M.M. And Nagro, S.A., 2024. Systematic Analysis Of Risks In Industry 5.0 Architecture. Applied Sciences, **14**(4), Pp. 1466.
[27] Muhammad, F.S., Lubis, M. And Fakhrurroja, H., 2023. Counterattacking Cyber Threats: A Framework For The Future Of Cybersecurity. Sustainability, **15**(18), Pp. 13369.
[28] Pandey, S., Singh, R.K., Gunasekaran, A. And Kaushik, A., 2020. Cyber Security Risks In Globalized Supply Chains: Conceptual Framework. Journal Of Global Operations And Strategic Sourcing, **13**(1), Pp. 103-128.
[29] Parsons, E.K., Panaousis, E., Loukas, G. And Sakellari, G., 2023. A Survey On Cyber Risk Management For The Internet Of Things. Applied Sciences, **13**(15), Pp. 9032.
[30] Pdf, 2024. A Raise Of Security Concern In Iot Devices: Measuring Iot Security Through Penetration Testing Framework. International Journal Of Advanced Computer Science And Applications, **15**(5),.