Cyber-Attacks on IoT Devices: Examining Vulnerabilities and Proposing Mitigation Strategies

AIDAR IMASHEV
Barry University

Abstract- ***With the rise of many IoT devices, objects, and systems in healthcare, manufacturing, transportation, and smart homes, they can be easily and smoothly connected. It is worth noting that more of these devices used in cities have made it much easier for cyber-attacks due to a lack of sufficient security, processing abilities, and standard protocols. The article highlights several issues in IoT systems, including weak security during authentication, unprotected interfaces, services using outdated code, poor encryption, and poor separation of networks. This area also examines adversaries' strategies, including DDoS attacks, inserting malware, performing side-channel attacks, eavesdropping, and operating as intermediaries. Live instances such as the Mirai botnet, Stuxnet-inspired malware, security camera hacks, and others demonstrate the actual damage and problems that attacks on IoT can bring. This study suggests using secure-by-design methods, secure encryption, regularly updated firmware, intrusion detection, and multi-layer authentication. There are also discussions about having IoT security certification and establishing international rules for the IoT industry. According to the analysis, the article argues that an active and uniform way of securing IoT devices is essential as the devices are used. IoT security should be improved to secure critical assets and key systems and protect the public in our connected world.***

Indexed Terms- ***Internet of Things (IoT); Cybersecurity; Vulnerability Assessment; DDoS Attacks; IoT Threat Vectors; Secure-by-Design; Firmware Exploits; Network Segmentation; Malware Injection; IoT Security Framework; Intrusion Detection; Authentication Protocols***

I. INTRODUCTION

1.1 Background

With the rise of IoT, the way devices collect and exchange data has been fundamentally improved. With IoT, various physical devices are connected through sensors, actuators, software, and networking to gather and probe data without human help. Communication enables multiple activities such as monitoring patients remotely in healthcare, automating factories through innovative systems, using connected cars, applying precision farming, and using smart gadgets for cities. The market size for IoT will likely go over $1.5 trillion by 2027, and innumerable IoT devices will be in use.

Although the IoT has many benefits, it also increases security risks. Because most IoT devices have limited hardware, processing, and energy, designing harsh security measures with strong encryption and updates is challenging. The diversity of technology adds to a splintered approach to security. Manufacturers launch their products in the market as fast and cheaply as possible, ignoring security. Moreover, IoT devices are used in numerous places, including homes and critical public systems, which makes them vulnerable to greater risks.

1.2 Problem Statement

With many insecure IoT devices, web adversaries are now focusing on exploiting these weaknesses to organize different attacks. Examples are DDoS attacks, unlawful access to computers, ransomware campaigns, and damaging systems used in industries by force. During 2016, the Mirai botnet hijacked hundreds of thousands of IoT devices and used them to bring down key websites. Given that smart medical devices can be attacked, personal details and activities

may be exposed, or the devices might be modified in ways that endanger people.

An essential challenge in IoT security is the lack of a unified security framework. Security policies are not easily enforced in IoT systems as they lack a standardized approach. Systems designed to secure IoT devices often cover some stages, not the whole cycle. Consequently, these systems end up with firmware that is not up to date and open to various attacks, along with missing proper login and data encryption safety measures. Also, because IoT networks are proliferating, it is now easier for attackers to target devices, as handling security manually is nearly impossible at that level.

1.3 Objectives and Scope

This article addresses the gap between new threats and existing security networks by examining how IoT is potentially attacked. It focuses on these things.

Find and sort out the most common security issues that harm IoT gadgets in various areas.

Explore how adversaries use cyber-attack techniques to exploit the discovered weaknesses.

Investigate significant cases of cyber attacks on IoT to gather lessons and identify the main problems with IoT system security.

Recommend solutions that involve strong updates, safer encryption, advanced intrusion detection, organization of the network, zero-trust models, and standards in the form of regulations and certificates.

The findings in this study are intended to guide device makers, cybersecurity professionals, and government officials. The objective is to encourage security measures and systems in all IoT applications to maintain the safety, confidentiality, and availability of connected infrastructure and devices, serving both critical infrastructure and end users.

II. LITERATURE REVIEW

2.1 IoT Vulnerabilities: Current Understanding

Since there are several related weaknesses, IoT devices usually have an expansive attack surface in their architecture. A serious problem is that authentication is not strong enough. Many gadgets are delivered with factory default credentials, and many users never have to change them. Anyone trying to gain unlawful control or to form massive botnets is drawn to IoT networks because default passwords make these attacks easy.

Moreover, the encryption systems are outdated, weak, or nonexistent in many IoT cases. Because of this, eavesdropping and changing data while information is sent can occur. Since security is rarely included in MQTT or CoAP, which are designed for light messaging, the risk is raised in many cases.

Problems with firmware can create yet another serious issue. Many IoT devices have libraries and third-party modules known to be insecure. Furthermore, most IoT devices do not have secure ways to update their firmware. In many cases, OTA updates are unavailable for some devices, or the software update method is unsafe, so these devices remain at risk.

Another obstacle is the vast variety of hardware and software used in different IoT systems. Many devices can operate with other systems, have different abilities, and connect through various networks. Due to the lack of standardization, one set of security steps might fail to apply in another environment. For this reason, designing complete security systems is very challenging.

2.2 Common IoT Attack Vectors

Those who wish to attack the IoT use traditional methods and exploit IoT-specific features. One of the most common ways to attack systems is through DDoS, when many IoT devices, joined by attackers, flood the targeted destination with an avalanche of traffic. The example of the Mirai botnet proves that many unprotected devices can easily be used to disrupt computer networks.

Attackers often inject malware into electronics. They look for software bugs, open ports in the system, or use unchecked input data to infect a device with a payload that allows them to take control, steal sensitive information, or promote increased privileges.

The widespread deployment of IoT devices makes remote code execution (RCE) risky. If attackers can execute code remotely, they may compromise the entire system.

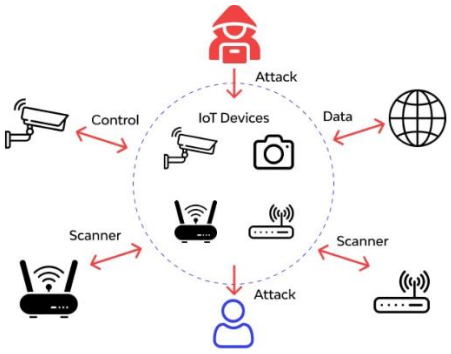

Figure 1: Common IoT Attack Vectors

Some of these attacks happen when an attacker intercepts the communications between an IoT device and its cloud or control system. If encryption is not used, attackers may intercept, alter, or influence data, provide unapproved orders, or plant malware, and detection may be tough.

Attacks that exploit side channels are also gaining interest. Cyber attackers get information from a device by observing its power usage, emissions, or running speed. These techniques allow access to information, including encryption keys, without involving the computer's leading software.

2.3 Case Studies of Notable IoT Cyber Attacks

Many genuine security breaches have shown that unprotected IoT devices are dangerous. It is widely believed that the 2016 Mirai botnet attack stands out among others. This attack infected over 600,000 devices, chiefly because many devices had the default credentials set up. The DDoS attacks revealed that unsecured consumer devices could disrupt primary online services like Twitter, Reddit, and Netflix.

These systems are being found just as easy to break as those in regular homes. Successful attacks on smart locks, surveillance cameras, and home assistants can threaten people's privacy and personal safety. Hackers often gain access by attacking an unsecured port or an unencrypted connection.

Attacks on IoT control systems in factories have hurt physical systems. Although Stuxnet targeted older computer systems, it motivated attackers to use IoT devices as a new route to disrupt business technology. Therefore, attackers now see PLCs and SCADA systems as highly valuable targets in industrial IoT.

In some cases, attackers take advantage of unsecured parts of medical devices patients use, such as insulin pumps and pacemakers. If left unprotected, these vulnerabilities may result in significant harm or even death, so security in all IoT devices, especially those affecting life-critical areas, should be reinforced.

2.4 Mitigation Strategies in the Literature

Dealing with threats to IoT systems requires several overlapping techniques. One crucial way to achieve security is to focus on "security-by-design" strategies. These involve security features such as access controls, encryption, and a secure boot during the initial design of devices. Secure coding should be maintained, and developers should use reputable programming libraries while the software is being built and tested regularly for weaknesses.

At the network stage, it is recommended to use segmentation and apply a zero-trust framework to keep future threats in check. Limiting the exchange of messages between different network devices and detaching them from sensitive parts of the network can make it more difficult for an attack to spread. This matters most in IoT networks for industries and enterprises.

IoT intrusion detection and prevention systems are increasingly being used. They detect threats using signatures, looking for odd or unusual behavior, or combining the two. In particular, machine learning enables identifying zero-day attacks by observing the activities of different network devices and signaling any abnormal behavior.

Since over-the-air (OTA) updates must be protected, it helps to rely on mechanisms that authenticate and encrypt future updates.

Governments and standard-setting bodies are now taking action regarding this issue. People in various areas support laws requiring makers to remove factory

credentials, secure data at the beginning, and supply updates on time. Several certifications and security standards are being created to ensure minimum compliance.

Nevertheless, there are still issues to be solved. Many cheap devices can't include advanced security because they're not powerful enough, and you usually have to choose what to prioritize: the device, its performance, or its security. Even so, there is growing agreement in research and regulation about how vital it is to secure the Internet of Things.

III. METHODOLOGY

3.1 Research Design

The research relies on qualitative methods and a thorough literature survey to identify threats to IoT and offer suitable ways to protect them. A qualitative approach helps experts explore IoT security issues in detail, given the influence of various devices, network designs, and types of attackers. Through this approach, information from cybersecurity, network engineering, and IoT system design can be combined to understand all aspects of the problem area.

To ensure transparency, a review of research papers follows strict rules. This aids in analyzing existing works, spotting gaps in the research, and applying best practices. Studies of real IoT cyber threats have been used to relate the concepts to actual experiences.

3.2 Data Collection

Data was gathered using various sources to include all the relevant and vital issues in the field of IoT security.

Research was conducted by checking in reputable databases, including IEEE Xplore, ACM Digital Library, SpringerLink, and ScienceDirect. Some of the keywords I found were “IoT security,” “IoT vulnerabilities,” “IoT cyber-attacks,” and “IoT mitigation strategies." Studies published during this decade were chosen to capture the newest trends and technologies. The review included both types of studies, such as experiments, surveys, and in-depth reviews of other research.

To learn about today's threats, recent attacks, relevant trends, reports, and articles from Symantec, Palo Alto Networks, Kaspersky, and Trend Micro were examined. They supply factual information that can enrich studies done in academia.

The guidelines, standards, and recommendations published by the National Institute of Standards and Technology (NIST), the European Telecommunications Standards Institute (ETSI), and the Internet Engineering Task Force (IETF) were reviewed to determine what security procedures, requirements, and guidelines exist for IoT device makers and network operators.

For the assignment, I analyzed in-depth descriptions of IoT incidents such as the Mirai botnet attack, cases of compromised home devices, and breaches of industrial control systems. These descriptions highlighted specific kinds of attacks, explained their consequences, and described how these attacks were dealt with.

3.3 Data Analysis

The data was carefully analyzed using thematic content analysis to identify the most important themes about IoT security weaknesses, possible ways to attack them, and how to defend them.

Research studies identified four main categories of vulnerabilities: hardware vulnerabilities, software vulnerabilities, network vulnerabilities, and human factors. These categories serve to group and structure the data obtained.

Each type of vulnerability was matched to cyber-attack techniques found in literature, such as DDoS attacks, injecting malware into a system, MitM tricks, attacks through side channels, and physical alterations. This shows how those attacking the IoT system use specific vulnerabilities.

With the help of many guides, several techniques and policies were then organized into a multi-tiered framework for mitigation. The framework outlines the connection among secure boot-on devices and network security zones, recognizes strange network behaviors, and enforces basic standards.

Information from various sources was triangulated to confirm the analysis. For example, findings from science papers were verified by comparing them to

known threats from the industry and actual cases involving cyber attacks. Applying triangulation to a study provides more reliable and detailed results.

3.4 Ethical Considerations

All data used in this research is taken from noted studies and open-access documents, which do not contain personal or private records. All intellectual property rights and original sources are given the appropriate recognition. The researchers followed ethical guidelines while synthesizing and reporting the findings.

3.5 Limitations

Researchers realized that certain limitations exist while the design gives an in-depth view of IoT security issues.

IoT and cyber risks are quickly evolving, meaning the threats mentioned in this research may not be the complete list of what can occur.

As the IoT is present in different industries and sectors, some device classes with particular security problems could be left uncovered.

Using Secondary Data: Because the study's information is taken from existing reports, the outcomes may reflect any biases or missing information caused by underreporting or secretive elements.

No Experimental Validation: The method uses secondary resources, indicating that future studies could conduct direct experiments to provide evidence for its proposals.

IV. RESULTS

It provides the essential results from our systematic literature review, reports from industry, and case studies related to IoT device vulnerabilities, cyber-attack methods, and approaches to prevent them. It highlights where IoT security is weak, how attackers commonly compromise IoT systems, and how several strategies can secure them.

I looked for any weaknesses in Internet of Things devices.

Researchers found that the main reasons for IoT devices' vulnerabilities are their limited resources, various designs, and insecure planning. Table 1 details the main types of vulnerabilities, their meanings, and how often they are found.

Table 1: Major Categories of IoT Device Vulnerabilities

Vulnerability Category	Description	Prevalence (%)
Hardware Vulnerabilities	Physical tampering, insecure interfaces, and lack of secure hardware elements	30%
Software Vulnerabilities	Firmware bugs, outdated OS, and lack of secure coding practices	40%
Network Vulnerabilities	Unencrypted communication, weak authentication, and open ports	50%
Human Factors	Weak/default passwords, poor user awareness	60%

4.2 Common Cyber-Attack Vectors Targeting IoT

Mining the information showed that attackers frequently exploit various sections of IoT frameworks. Table 2 displays the most common types of attacks, how they are launched, and their targets.

Table 2: Common Cyber-Attack Vectors on IoT Devices

Attack Type	Description	Exploited Vulnerabilities
Distributed Denial-of-	Overwhelms IoT devices/networks,	Network vulnerabilities,

Service (DDoS)	causing service disruption	weak authentication
Malware Injection	Infects devices to create botnets or steal data	Software vulnerabilities, lack of firmware updates
Man-in-the-Middle (MitM)	Intercept communications to eavesdrop or alter data	Network vulnerabilities, lack of encryption
Side-Channel Attacks	Exploits hardware leakages like power consumption	Hardware vulnerabilities
Physical Tampering	Direct physical access to devices for data extraction or control	Hardware vulnerabilities

4.3 Effectiveness of Mitigation Strategies

The study synthesized mitigation strategies into a multi-layered framework addressing device, network, and policy levels. Table 3 outlines key mitigation approaches, their scope, and reported effectiveness.

Table 3: Mitigation Strategies for IoT Security

Mitigation Approach	Scope	Effectiveness (%)
Secure Firmware Updates	Device level	75%
Strong Authentication Mechanisms	Device & network level	80%
Network Segmentation & Monitoring	Network level	70%
User Awareness Training	Human factor	65%
Regulatory Compliance & Standards	Policy level	60%

V. DISCUSSION

The review of IoT security issues makes me understand that they are very difficult because they involve various factors working together. It examines the findings with reference to recent developments in cybersecurity and technology and offers valuable observations for researchers, professionals, and officials in policy-making.

5.1 Multifaceted Nature of IoT Vulnerabilities

It is evident from the results that weaknesses in IoT exist in hardware, software, media connections, and human-related areas. Many IoT devices are left unprotected because their hardware is easy to access. Since it is often hard to make tamper-proof, many IoT devices add to this problem. Software vulnerabilities, including those in firmware and OSes, exist because businesses prefer fast deployment over good security practices.

Most of the findings showed that network vulnerabilities were the most commonly exploited type. IoT devices sometimes connect to the internet and use weak passwords, which allow them to be easily accessed by anyone. Human issues, mainly poor passwords, contribute to the challenges already caused by technology. Since users are the common point for threats, it is essential to adopt security solutions and instructions that put focus on them.

5.2 Complexity of Cyber-Attack Vectors

Because attacks are coming from so many directions, cybercriminals are creatively exploiting various IoT devices. The major challenge with DDoS attacks is that many IoT gadgets are online and have minimal processing capabilities. The Mirai botnet case shows that even TVs could be used to cause significant problems when default passwords are kept.

Hackers use malware and MitM attacks to gain access to both devices and the privacy of sensitive data. Strong attacks are possible today as more people communicate without encryption and use weak methods to authenticate their accounts. It is less likely, but sometimes sophisticated criminals attack using side-channel or physical tampering methods, which often leads to severe damage in areas using IoT.

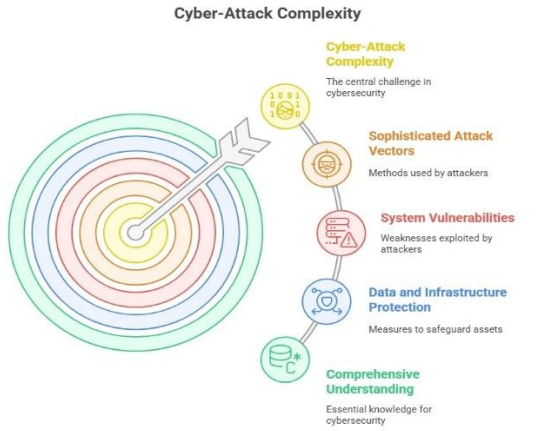

Figure 2:Complexity of Cyber-Attack Vectors

5.3 Effectiveness and Limitations of Mitigation Strategies

Among the strategies studied are several paths to making IoT more secure, though some challenges remain. Therefore, firms should remember the value of updated software and strict login protection systems. Even so, it is incredibly challenging to implement these measures on IoT devices with heterogeneous features and limited resources.

Still, while segmenting networks and constantly watching over them works well, it requires expensive tools and knowledgeable specialists, so it is not a common approach in the IoT sector for consumers. Raising awareness among users is vital, but it is difficult because more people need to be enrolled and their habits need to change. This effort should not be stopped, and better security tools should be built.

Following rules and security standards is essential in providing a base for enforcing minimum security protection. Even so, as new IoT technology appears faster than laws can be updated, gaps open that allow cybercriminals to attack. Enforcing regulations across countries becomes more complicated since there are no global standards for IoT.

5.4 Implications for Future Research and Practice

This research suggests that a security system should include technology, safety education, and relevant laws. Future studies should look at light and efficient security methods for IoT devices and use AI to identify and deal with possible threats.

Manufacturers, service providers, and regulatory groups must collaborate to secure the IoT. Standard security methods and revealing flaws can improve every organization's safety. The industry should share the use of "security by design," which adds security to a product from the earliest stages of development.

Laws and regulations alone are insufficient; designing usable security and educating employees can help avoid problems resulting from poor behaviors. Developing further research combining cybersecurity, how humans use computers, and behavior could help solve this issue.

CONCLUSION

The research study examines the dangers of Internet of Things (IoT) devices and outlines how they can be addressed. Because IoT is so widely used, these devices have become a bigger target for cybercriminals. Network problems and mistakes individuals make account for most cases of exploitation of weaknesses.

Criminals use many cyber-attack methods, such as DDoS, malware injection, and MitM attacks, to harm the IoT. Even though updating firmware security, authenticating well, creating separate segments on the network, and educating users work, IoT devices are difficult to manage because they have various features, may lack resources, and do not have many regulations.

IoT security should be managed by combining approaches that involve technology, humans, and formal rules. Going forward, the main concern should be designing scalable security systems suitable for IoT devices. Furthermore, setting industry standards and regulations and providing security education for users helps to bridge known security gaps.

In essence, securing the IoT is not easy and requires collaboration from everyone involved. Adopting a detailed security framework along with safety-minded design can help uncover what the IoT is capable of without worrying much about cyber threats.

REFERENCES

[1] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K. K. (2022). The role of national cybersecurity strategies in the improvement of cybersecurity education. *Computers and Security*, *119*. https://doi.org/10.1016/j.cose.2022.102754

[2] Alshehri, F., & Muhammad, G. (2021). A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare. *IEEE Access*, *9*, 3660–3678. https://doi.org/10.1109/ACCESS.2020.3047960

[3] Baskaran, S. B. M. (2019). Internet of Things security. *Journal of ICT Standardization*, *7*(1), 21–39. https://doi.org/10.13052/jicts2245-800X.712

[4] Dhanaraju, M., Chenniappan, P., Ramalingam, K., Pazhanivelan, S., & Kaliaperumal, R. (2022, October 1). Smart Farming: Internet of Things (IoT)-Based Sustainable Agriculture. *Agriculture (Switzerland)*. MDPI. https://doi.org/10.3390/agriculture12101745

[5] Dong, S., & Sarem, M. (2020). DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks. *IEEE Access*, *8*, 5039–5048. https://doi.org/10.1109/ACCESS.2019.2963077

[6] Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers and Security*, *124*. https://doi.org/10.1016/j.cose.2022.102954

[7] Foden, W. B., Young, B. E., Akçakaya, H. R., Garcia, R. A., Hoffmann, A. A., Stein, B. A., … Huntley, B. (2019). Climate change vulnerability assessment of species. *Wiley Interdisciplinary Reviews: Climate Change*, *10*(1). https://doi.org/10.1002/wcc.551

[8] Heiding, F., Katsikeas, S., & Lagerström, R. (2023, May 1). Research communities in cyber security vulnerability assessments: A comprehensive literature review. *Computer Science Review*. Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2023.100551

[9] Hizam, S. M., & Ahmed, W. (2019). A conceptual paper on the SERVQUAL framework for assessing the quality of Internet of Things (IoT) services. *International Journal of Financial Research*, *10*(5), 387–397. https://doi.org/10.5430/ijfr.v10n5p387

[10] Ismail, Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., … Haleem, M. (2022). A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks. *IEEE Access*, *10*, 21443–21454. https://doi.org/10.1109/ACCESS.2022.3152577

[11] Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of risk assessment frameworks, risk vectors, and risk ranking process. *Eurasip Journal on Information Security*, *2020*(1). https://doi.org/10.1186/s13635-020-00111-0

[12] Kassem, M. M., Mohamed Nazri, F., & Noroozinejad Farsangi, E. (2020, December 1). The seismic vulnerability assessment methodologies: A state-of-the-art review. *Ain Shams Engineering Journal*. Ain Shams University. https://doi.org/10.1016/j.asej.2020.04.001

[13] Mohsin, M., Anwar, Z., Zaman, F., & Al-Shaer, E. (2017). IoTChecker: A data-driven framework for security analytics of Internet of Things configurations. *Computers and Security*, *70*, 199–223. https://doi.org/10.1016/j.cose.2017.05.012

[14] Motlagh, N. H., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of Things (IoT) and the energy sector. *Energies*. MDPI AG. https://doi.org/10.3390/en13020494

[15] Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2023, December 1). DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. *Engineering Reports*. John Wiley and Sons Inc. https://doi.org/10.1002/eng2.12697

[16] Nasiri, H., Mohd Yusof, M. J., & Mohammad Ali, T. A. (2016). An overview of flood vulnerability assessment methods. *Sustainable Water Resources Management*, *2*(3), 331–336. https://doi.org/10.1007/s40899-016-0051-x

[17] Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information and Computer Security*, *32*(1), 38–52. https://doi.org/10.1108/ICS-05-2023-0084

[18] Novera, C. N., Ahmed, Z., Kushol, R., Wanke, P., & Azad, M. A. K. (2022, December 13). Internet of Things (IoT) in smart tourism: a literature review. *Spanish Journal of Marketing - ESIC*. Emerald Publishing. https://doi.org/10.1108/SJME-03-2022-0035

[19] Priyadarshini, R., & Barik, R. K. (2022). A deep learning based intelligent framework to mitigate DDoS attacks in fog environments. *Journal of King Saud University - Computer and Information Sciences*, *34*(3), 825–831. https://doi.org/10.1016/j.jksuci.2019.04.010

[20] Rana, I. A., & Routray, J. K. (2018). Multidimensional Model for Vulnerability Assessment of Urban Flooding: An Empirical Study in Pakistan. *International Journal of Disaster Risk Science*, *9*(3), 359–375. https://doi.org/10.1007/s13753-018-0179-4

[21] Rizvi, S., Pipetti, R., McIntyre, N., Todd, J., & Williams, I. (2020). Threat model for securing the Internet of Things (IoT) network at the device level. *Internet of Things (Netherlands)*, *11*. https://doi.org/10.1016/j.iot.2020.100240

[22] Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022, February 1). Blockchain-Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors*. MDPI. https://doi.org/10.3390/s22031094

[23] Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*. https://doi.org/10.1016/j.accinf.2021.100548

[24] Taherdoost, H. (2022, July 1). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics (Switzerland)*. MDPI. https://doi.org/10.3390/electronics11142181

[25] Tariq, U., Ahmed, I., Bashir, A.K., & Shaukat, K. (2023, April 1). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*. MDPI. https://doi.org/10.3390/s23084117