IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11701

IoT Device Security and Network Protocols: A Survey on the Current Challenges, Vulnerabilities, and Countermeasures

Okereke George E. [1], **Mathew Daniel E.** [2], **Ukeoma Pamela E.** [3], **Uzo Blessing C.** [4], **Umaru Adanu A.** [5], **Dibiaezue Ngozi F.** [6]

Computer Science Department, University of Nigeria, Nsukka (UNN), Nigeria[1]

Centre for Atmospheric Research, National Space Research and Development Agency, Anyigba[2]

Computer Science Department, University of Nigeria, Nsukka (UNN), Nigeria[2]

Computer Science Department, University of Nigeria, Nsukka (UNN), Nigeria[3]

Computer Science Department, University of Nigeria, Nsukka (UNN), Nigeria[4]

Computer Science Department, University of Nigeria, Nsukka (UNN), Nigeria[5]

Computer Science Department, University of Nigeria, Nsukka (UNN), Nigeria[6]

Abstract: This survey delves into the critical domain of IoT device security and network protocols, examining prevailing challenges, vulnerabilities, and countermeasures. As IoT devices proliferate across diverse sectors, ensuring their security becomes paramount, necessitating a comprehensive exploration of existing challenges. The study scrutinizes the vulnerabilities associated with current IoT network protocols, shedding light on potential threats and weaknesses. By providing an in-depth analysis of countermeasures, the paper seeks to contribute valuable insights into fortifying the security posture of IoT devices and their underlying network infrastructure. This comprehensive survey serves as a useful resource for researchers, practitioners, and policymakers aiming to address the evolving landscape of IoT security.

Key Words: IoT device, network protocols, challenges, vulnerabilities, countermeasures.

I. INTRODUCTION

Securing Internet of Things (IoT) devices and network protocols emerged as a paramount concern in our increasingly connected world. As the IoT ecosystem expands, with billions of smart devices being deployed in various sectors, ranging from healthcare to industrial automation, the need for robust security measures is more critical than ever. Sensors, actuators, and smart appliances, constituting IoT devices, have seamlessly woven into our everyday routines, providing convenience and enhancing efficiency. However, their proliferation has also attracted the attention of malicious actors, who seek to exploit vulnerabilities in these devices and the protocols that underpin their communication. Securing IoT devices and networks requires a multi-layered approach, combining technical and non-technical measures. Consistent security audits and staying abreast of emerging threats and vulnerabilities are crucial for upholding a robust security stance in the dynamically changing IoT environment.

The challenges in securing IoT devices and network protocols are multifaceted. IoT devices often come with resource constraints, limiting the implementation of traditional security measures. Moreover, the sheer diversity of devices, with unique characteristics and potential vulnerabilities, complicates the security landscape. Additionally, many IoT networks span a vast array of communication protocols, some of which may lack robust security features, leaving them susceptible to attacks. According to [1] the exposure of objects migrating to the internet to attacks from unauthorized devices necessitates the development of secure protocols or the addition of security features to existing ones, with a focus on minimizing overhead and addressing vulnerabilities in routing, given the limitations of current security mechanisms for small constrained objects. The vulnerabilities that IoT ecosystems face are varied and can have far-reaching consequences. Insecure authentication mechanisms, inadequate encryption, and vulnerabilities in firmware updates are just a few examples. Exploiting these vulnerabilities may result in unauthorized access, data breaches, or the compromise of entire networks, posing potential risks to user privacy, data integrity, and even physical safety.

DOI: 10.17148/IARJSET.2024.11701

To address these challenges and vulnerabilities, organizations and manufacturers are increasingly focusing on the development of comprehensive security strategies, incorporating encryption, authentication, and access control measures into IoT devices and networks. This comprehensive strategy seeks to guarantee the confidentiality, integrity, and availability of IoT systems. Additionally, regulatory bodies and industry standards are playing an essential role in shaping the security landscape of IoT, enforcing compliance with data protection regulations, and promoting secure-by-design principles. The work of [2] shows the extensive scope of IoT security that spans four dimensions, encompassing tasks often overlooked like privacy, computation, trusted sensing, communication, and digital forgetting, demanding innovative techniques to safeguard hardware, software, and data, especially considering potential physical access to IoT devices, with additional challenges arising from the security of sensors and actuators, including the integrity of physical signals and actuating events.

Studies have shown that enough has not been done to cover this emerging field of high-performance intelligence computing. Therefore, this exploration on securing IoT devices and network protocols has become very vital to serve as a guide to all concerned in the emerging growth in the deployment and security of IoT devices, network protocols, and cloud computing technology with a main focus on the key security principles, challenges, vulnerabilities, and countermeasures that are shaping the landscape of IoT security in ensuring a safer and more reliable future for this rapidly evolving technology which has not been deeply dealt with in so many work reviewed. The next section of this work is the review of some related works on securing IoT and network protocols. Thereafter, we considered some common security challenges, vulnerabilities, and countermeasures. The final section of the paper covered the contribution to knowledge, future areas of study that are recommended, and the conclusion drawn from the work.

II. RELATED REVIEWED

The Internet of Things (IoT) stands as a transformative technological progression affecting diverse sectors like industry, environmental care, medicine, and urban development; however, it encounters challenges including technology interoperability, data confidentiality, security, and the implementation of energy-efficient management systems. The study conducted by [3] thoroughly investigates networking communication technologies for IoT, with a focus on encapsulation and routing protocols, delivering a detailed layer-based protocol taxonomy, and elucidating the internal schemes and mechanisms of IPv6-related network protocols, setting it apart from other survey works. The discussion also delves into compatibility, interoperability, and configuration issues, addressing open challenges like security, scalability, mobility, and energy management, while outlining future trends in IoT networking mechanisms. The survey presented in [4] thoroughly examines the security of application layer protocols in IoT environments, specifically those concerning messaging/data sharing and service discovery. It underscores the intricate nature of the threat landscape and scrutinizes the primary challenges, vulnerabilities, and proposed security measures. The results underscore the challenges in ensuring security at the application layer, emphasizing the exposure of IoT devices to various risks arising from inadequate security services in protocols, vulnerabilities, and limitations in device capabilities.

As indicated by [5], the Internet of Things (IoT) or Web of Things (WoT) establishes a wireless network that links smart products to the Internet, enabling the incorporation of numerous gadgets and devices. The swift expansion of this market gives rise to security apprehensions, prompting the creation of IoT protocols such as 802.15.4, 6LoWPAN, and RPL for diverse layers. Additionally, the adoption of CoAP (Constrained Application Protocol) as an application layer protocol is noteworthy, and this study specifically focuses on addressing security issues in CoAP over DTLS, presenting solutions, and identifying future research challenges. Similarly, [6] conducts a survey on the security aspects of four commonly used IoT protocols, namely Bluetooth Low Energy, LoRaWAN, ZigBee, and Z-Wave, highlighting vulnerabilities and tracing the evolution of these protocols from a security perspective, laying the groundwork for future research focused on developing a secure gateway for IoT networks capable of detecting security incidents at the interface connecting IoT devices and application servers. While [7] provides a comparative analysis of IoT protocols utilized for data transfer in constrained IoT networks, acknowledging the challenges of setting up networks with numerous physically interconnected IoT devices. Focusing on efficient M2M (Machine to Machine) communication in constrained networks, the study evaluates and compares the performance of MQTT (Message Queuing Telemetry Transport) and CoAP protocols in various scenarios to aid in the challenging task of protocol selection during the development of IoT applications.

The significant role of IoT in handling extensive data from diverse devices, employing machine learning and data analytics algorithms for information extraction and event prediction, while addressing the notable challenge of secure information routing over the internet with limited resources [8]. The main emphasis of the survey is to examine the research challenges and unresolved issues concerning IoT security and protocols, contributing by spotlighting research trends and the utilization of simulation tools in analyzing IoT layer protocols. The evaluation conducted by [9] on the security framework of the Internet of Things (IoT) presents a detailed categorization of primary challenges in the domain.

DOI: 10.17148/IARJSET.2024.11701

It delves into key technologies such as Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN), crucial contributors to IoT development. The review explores relevant protocols for IoT infrastructure, emphasizes open-source tools and platforms, and concludes with a concise summary of prevailing challenges, possible solutions, and future research directions in the field. The study conducted by [10] presents System IDentifier (SysID), an automated system designed to classify device characteristics by analyzing their network traffic using a single packet originating from the device. Employing genetic algorithms (GA) to identify pertinent features in protocol headers and utilizing various machine learning (ML) algorithms, SysID achieves a classification accuracy exceeding 95%, showcasing its fully automated capability without the need for expert input. This was demonstrated through an experimental study involving 23 IoT devices.

Research by [11] was a dual-pronged approach, addressing the challenges of defining a generic method for comparing IoT protocol stacks based on criteria such as range, openness, interoperability, topology, and security practices, while also proposing a generic way to describe fundamental IoT attacks irrespective of the protocol, categorizes attacks into three parts: packet-focused attacks (passive and active cryptographic attacks), protocol-focused attacks (MITM, Flooding, Sybil, Spoofing, Wormhole attacks), and system-focused attacks (Sinkhole, Selective forwarding attacks), emphasizing commonalities among different IoT protocols and identifying mechanisms that render them vulnerable to specific attacks. The Internet of Things (IoT) enables the linking of intelligent physical and virtual objects, specifically constrained devices constrained by limitations in energy, computing, and storage capacity. In the realm of Wireless Sensor Networks (WSN), overseen by a Personal Area Network Coordinator (CPAN) and recognized for low bit rate and power consumption, [12] presents a sturdy, streamlined, and energy-efficient security protocol. This protocol ensures mutual authentication, encryption, and authentication of exchanged data when integrating new devices, accompanied by real tests and performance evaluations.

According to [13], the growing abundance of IoT devices and applications underscores the importance of enhancing the security capabilities of current protocols and networking stacks. This includes those specified by acknowledged standardization bodies like IEEE and IETF, along with industry alliances such as NFC Forum, ZigBee Alliance, Thread Group, and LoRa Alliance. The emphasis is on the significance of standardized and interoperable security solutions to safeguard IoT systems from malicious attacks and thwart unauthorized control over devices. The complexity of designing and implementing security policies for the expansive and resource-constrained Internet of Things (IoT) network was explored by [14] that provides an overview of the IoT protocol stack, analyzes commonly used protocols, and offers a security-focused comparison, while also addressing challenges related to security in terms of protocols, network, and devices. In [15], a classification system for security protocols in the Internet of Things (IoT) is delineated, covering critical elements such as key management, user and device authentication, access control, identity management, and privacy preservation. Subsequently, there is a comparative examination of modern IoT-related security protocols, considering their supported security and functionality features. The paper concludes with a discourse on upcoming challenges within the domain of IoT security protocols.

III. SECURITY CHALLENGES, VULNERABILITIES, AND COUNTERMEASURES

According to [16, 26,27] IoT is an indispensable component of contemporary industrial, agricultural, healthcare, and smart city advancements and requires comprehensive security measures due to widespread data collection and broadcasting, while current protocols operate with IP as a backbone and ensure security at multiple layers that focus on specific IoT protocols dedicated to securing IoT networks. Securing IoT devices and the network protocols they use is crucial to prevent cyberattacks, data breaches, and unauthorized access to connected devices. Table 1 contains some security issues, stating their descriptions, challenges, vulnerabilities, and countermeasures:

TABLE 1: Some IoT Device Security and Network Protocols Challenges, Vulnerabilities, And Countermeasures

S/N	Security Threats	Description	Challenges	Vulnerabilities	Countermeasures	Authors
1.	Device Authentication	Device authentication is crucial for IoT and network protocol security, ensuring device	i. Managing authentication for numerous IoT devices is complex and resource-intensive. ii. Many IoT devices have weak or default	i. Inadequate authentication mechanisms enable unauthorized access to IoT devices. ii. Weak or default passwords are	i. Implement strong authentication methods like device certificates, biometrics, or multi-factor	[17], [28], [29], [30], [31], [32].

		identity and trustworthiness to protect ecosystems from physical and cloning attacks. Robust authentication methods and best practices are essential for mitigating vulnerabilities and maintaining trust in IoT networks.	passwords that users often don't change. iii. Limited processing power and memory hinder robust authentication on some IoT devices. iv. IoT devices needing remote authentication are vulnerable to attacks. v. Diverse authentication methods and protocols complicate standardizing IoT device authentication.	prone to brute-force attacks. iii. Man in the Middle (MitM) can attack authentication traffic, capturing sensitive information. iv. Locally stored credentials on IoT devices are susceptible to theft. v. Through eavesdropping where attackers listen on the authentication process and gather data.	authentication to secure IoT devices and networks. ii. Use public-key cryptography or multifactor authentication to enhance security. iii. Encourage regular password updates and strong password policies. iv. Securely store authentication keys within devices to prevent extraction. v. Use Identity and Access Management (IAM) systems to manage device identities, authentication, and authorization centrally and at scale.	
2.	Data Encryption	Data encryption is crucial for IoT security because it enhances data confidentiality and integrity, protecting against attacks and breaches. Unencrypted transmissions risk interception and eavesdropping.	i. IoT data encryption must comply with privacy regulations, complicating implementation. ii. Limited computational IoT devices hinder efficient encryption. iii. Secure key management for numerous IoT devices is complex and vulnerable. iv. Ensuring secure communication across IoT devices from different manufacturers using standardized encryption protocols is challenging.	i. Outdated or weak encryption algorithms create vulnerabilities exploitable by attackers. ii. Insufficient protection of encryption keys allows attackers to access them, compromising encryption. iii. Attackers intercept and alter encrypted data during transmission, risking data integrity and confidentiality. iv. Attackers exploit side-channel exposure to extract encryption keys, especially in resource-limited IoT devices.	i. Implement end-to-end encryption to ensure only authorized parties can decrypt data from source to destination. ii. Use modern algorithms like AES to protect data, avoiding outdated methods. iii. Use secure systems to generate, distribute, and store encryption keys, rotating them regularly. iv. Use Hardware Security Modules (HSMs) for top security, storing and managing encryption keys in a tamper-resistant way. v. Use network-level encryption protocols, to protect data in	[18], [33], [34], [35], [36], [37], [38], [39].

DOI: 10.17148/IARJSET.2024.11701

					transit between IoT devices and the cloud or other endpoints.	
3.	Firmware Updates	Firmware updates are crucial for IoT security, addressing vulnerabilities and improving device security, and secure protection for IoT devices commonly involves the implementation of firmware updates. However, traditional update methods face limitations like restricted bandwidth and potential exploitation. Strong authentication, encryption, and security practices are essential for maintaining IoT device integrity.	i. Verifying firmware updates is challenging for resource-constrained IoT devices. ii. Limited storage, processing power, and memory hinder effective firmware updates on many IoT devices. iii. Ensuring secure, reliable network connectivity for firmware updates is complex, especially in remote areas. iv. Attackers may exploit rollback exposures to revert devices to earlier, insecure firmware versions.	i. Unauthorized firmware updates can compromise security, leading to unauthorized access or hijacking. ii. Attackers may intercept and replace firmware updates with malicious versions or block updates during transmission. iii. Firmware updates may be vulnerable during the boot process. iv. Attackers can impersonate legitimate devices to obtain and install firmware updates.	i. Use code signing to verify firmware authenticity, ensuring it comes from a trusted source and is untampered. ii. Use TLS for secure communication between devices and update servers to protect updates in transit. iii. Secure the updated network with encryption, firewall rules, and intrusion detection to protect transmissions. iv. Maintain version control to ensure devices update to the latest authorized firmware, preventing rollback attacks.	[19], [40], [41], [42], [43], [44], [45].
4.	Access Control	Access control is vital in IoT to prevent unauthorized device and data access. Ensuring IoT trust relies on effective access control, with various models suited to IoT implementation . Addressing challenges and implementing robust measures enhances IoT ecosystem integrity and security.	i. There is complicating uniform access control in IoT ecosystems with varied devices with different capabilities. ii. Managing access control for numerous IoT devices and users is complex and resource-intensive. iii. Constantly changing IoT environments make enforcing access control rules challenging. iv. Ensuring access control mechanisms	i. Weak access control allows unauthorized devices to access sensitive data or systems. ii. Attackers can exploit weak or default device authentication methods. iii. Attackers may steal credentials, impersonating authorized devices. iv. Poor authorization policies can lead to unauthorized actions by	i. Implement strong authentication methods like biometrics to verify user and device identities. ii. Centrally manage device identities and permissions for consistent and secure access control across the IoT ecosystem. iii. Use centralized servers to manage access policies and monitor enforcement.	[20], [46], [47], [48], [49], [50], [51], [52].

DOI: 10.17148/IARJSET.2024.11701

		Inadequate access control can lead to unauthorized access or manipulation, highlighting the need for robust mechanisms and role-based privilege restrictions.	work across different IoT devices and platforms is difficult.	legitimate users or devices.	v. Implement logging and monitoring to detect and respond to unauthorized or suspicious activities.	
5.	Network Security Protocols	Securing network protocols in IoT is essential for safeguarding data and communications between devices and servers. Insecure or outdated protocols can expose devices to attacks. Addressing these challenges can enhance IoT data availability, integrity, and confidentiality, focusing on standardized communication protocols like Constrained Application Protocol and Message Queuing Telemetry Transport protocol.	i. Limited processing power and memory in many IoT devices can hinder the implementation of complex security protocols. ii. Diverse devices from various manufacturers with different protocols make security standardization difficult. iii. Compliance with data privacy regulations adds complexity to IoT network security. iv. Ensuring secure communication across diverse devices and platforms using standardized network protocols is challenging.	i. Insufficient encryption can make data vulnerable to eavesdropping during transmission. ii. Flaws in network security protocols can be exploited by attackers. iii. Attackers can intercept and alter data in transit, compromising its integrity and confidentiality. iv. Incorrect security settings or key management can create vulnerabilities.	i. Use firewalls and IDS to monitor network traffic for malicious activity. ii. Promote standardized network security protocols for consistency and interoperability. iii. Apply security measures across multiple IoT architecture layers, including application, transport, and network layers. iv. Enforce strong authentication and authorization controls to allow access only to authorized devices and users. v. Use network security protocols to secure firmware update delivery. Vi. Implement real-time monitoring and anomaly detection to identify potential compromises.	[21], [53], [54], [55], [56], [57], [58], [59].
6.	Intrusion Detection Systems	Intrusion Detection Systems (IDS) are crucial for safeguarding IoT networks and devices from security threats.	i. Complicating the creation of IDS rules and signatures in IoT ecosystems for various device types with unique communication protocols.	i. Inaccurate IDS alerts can cause numerous false positives, wasting resources and leading to alert fatigue. ii. Misconfigurations	i. Implement real-time monitoring to promptly detect and address threats. ii. Create custom IDS rules specific to IoT devices and protocols to	[60], [61], [62], [63], [64], [65], [66].

		Implementing IDS in IoT requires careful planning and adaptation to specific ecosystem challenges. Addressing these challenges enhances IDS's effectiveness in protecting IoT environments.	ii. Limited processing power and memory in many IoT devices make resource-intensive IDS solutions difficult to implement. iii. Essential for timely threat detection but challenging to implement due to resource demands in IoT environments. iv. IoT networks produce vast amounts of data, potentially overwhelming IDS solutions and causing false positives or missed alerts.	or incomplete rule sets can fail to detect real threats, leaving IoT systems exposed. iii. Attackers might flood an IDS with traffic to deplete its resources, making it ineffective. iv. Attackers may use specially crafted packets to evade IDS detection, exploit vulnerabilities, or conduct reconnaissance.	minimize false positives. iii. Use data aggregation and filtering to decrease the data volume IDS must process. iv. Employ protocol analysis to identify unusual or malicious network traffic patterns. v. Optimize IDS solutions for efficient operation on resource-limited IoT devices and networks.	
7.	Physical Security	Physical security in IoT is crucial for protecting devices from tampering, theft, and unauthorized access. Often overlooked in security literature, it addresses preventing vandalism and theft. Enhancing physical security ensures device availability and integrity, bolstering IoT services.	i. IoT devices' limited resources hinder the implementation of robust physical security measures. ii. Ensuring uniform physical security is challenging due to IoT devices being spread across various locations. iii. Devices face physical attack risks during manufacturing, shipping, or provisioning. iv. IoT devices in distant or unmanned locations are particularly vulnerable to physical attacks.	i. IoT devices can be stolen by unauthorized individuals, causing data loss and unauthorized access. ii. Attackers may physically alter IoT devices to extract sensitive information or disrupt functionality. iii. Genuine devices can be replaced with counterfeit ones, creating security risks. iv. Devices can be compromised during manufacturing or shipping, introducing vulnerabilities.	i. Secure IoT devices in protective enclosures or cabinets to prevent tampering and theft. ii. Track the location of IoT devices to deter theft or unauthorized movement. iii. Use sensors to detect changes in environmental conditions that may indicate tampering. iv. Limit physical access to IoT devices with mechanisms like card readers, biometrics, or keys. v. Apply tamper-evident seals or labels to device enclosures to identify tampering attempts.	[67], [68], [69], [70], [71], [72], [73], [74].

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⪤ Peer-reviewed & Refereed journal ⪤ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11701

8.	Privacy and Data Protection	Privacy and data protection are crucial for IoT security, ensuring sensitive information is managed carefully and in line with regulations. By tackling challenges and implementing appropriate countermeasures, organizations can improve data privacy, and security, and build user trust in IoT ecosystems.	i. IoT devices gather and transmit personal data, like health and location information, raising privacy concerns. ii. Securing stored data on IoT devices or in the cloud is challenging due to resource limits and encryption needs. iii. Managing informed consent for data collection and sharing is complex in large-scale IoT deployments. iv. Sharing data among manufacturers, service providers, and third parties increases the risk of unauthorized access.	i. Insufficient access controls may allow unauthorized entry to sensitive data, risking misuse or exposure. ii. Poor data protection may result in breaches, exposing sensitive information to unauthorized entities. iii. Weak or lacking encryption during data transmission and storage can jeopardize data, inviting theft or eavesdropping. iv. Intercepting data transmitted between IoT devices and the cloud can jeopardize data privacy.	i. Use end-to-end encryption to secure data during transit, ensuring access is limited to authorized parties. ii. Collect only necessary data to reduce the amount of sensitive information stored. iii. Securely store data using encryption, access controls, and hardware security modules (HSMs). iv. Anonymize or pseudonymize data to protect user identities while maintaining data utility. v. Employ strong user authentication to verify identities accessing IoT data.	[23], [25], [75], [76], [77], [78], [79], [80], [81].
9.	IoT Device Management	Effective IoT device management is important for securing and maintaining reliable IoT ecosystems. Poor management can lead to misconfigured or unpatched devices. Implementing centralized device management solutions allows organizations to monitor, update, and secure devices, mitigating potential risks.	i. The rapid increase in IoT devices complicates large-scale management. ii. Managing devices throughout their lifecycle, including provisioning, configuration, monitoring, and decommissioning, is complex. iii. Limited resources in many IoT devices hinder robust management capabilities. iv. Ensuring device management solutions are compatible with various devices and platforms is challenging.	i. Outdated firmware and software can leave devices vulnerable to known security threats. ii. Weak access controls can enable unauthorized users to manipulate devices or their settings. iii. Poor device management can lead to compromised devices, which may be used in botnets or attacks. iv. Misconfigurations or unauthorized access to management systems can result in data privacy breaches.	i. Implement robust access controls to ensure only authorized users and administrators can manage devices. ii. Ensure devices use secure boot processes to verify firmware integrity during start-up. iii. Use strong device authentication to verify the identity of devices connecting to management systems. iv. Support remote device management, allowing administrators to configure and update devices	[82], [83], [84], [85], [86], [87], [88], [89].

					without physical access.	
10.	Network Segmentation	Effective network segmentation enhances IoT security by limiting the attack surface and mitigating breach impacts. This fundamental practice involves dividing a network into smaller, isolated segments to improve overall security.	i. Segmentation of IoT networks can be complex, especially in diverse and large environments. ii. Limited processing power and memory in some IoT devices can make segmentation difficult. iii. Ensuring secure communication across segmented networks is challenging. iv. Maintaining and updating segmentation rules regularly is resource-intensive.	i. Poor segmentation can allow attackers to move between segments ("segment hopping"). ii. Misconfigured segmentation rules can cause unintended inter-segment communication, posing security risks. iii. Attackers can launch DoS attacks within segments, exhausting resources. iv. Vulnerabilities in gateway devices or connecting devices can lead to inter-segment attacks.	i. Follow a "Zero Trust" model, assuming no segment is inherently secure and requiring strict verification for all traffic. ii. Define clear segmentation policies specifying which devices can communicate and under what conditions. iii. Enforce robust access control at segment levels using firewalls, authentication, and authorization mechanisms. iv. Deploy IDS/IPS to monitor for unauthorized access to segments.	[90], [91], [92], [93], [94], [95], [96], [97],

IV. CONTRIBUTION TO KNOWLEDGE AND RECOMMENDATION FOR FUTURE STUDY

This survey explores the intricate terrain of IoT device security, with a specific emphasis on the related network protocols. It systematically identifies and analyzes the prevailing challenges encountered by IoT devices, bringing attention to vulnerabilities that could endanger the integrity, confidentiality, and availability of data within IoT networks. One significant contribution of the research lies in its meticulous examination of the various countermeasures employed to address the identified challenges and vulnerabilities of existing practices and solutions that offer a valuable resource for practitioners, researchers, and policymakers seeking a comprehensive understanding of the strategies available to enhance IoT device security which is vital in the face of the evolving threat landscape surrounding IoT ecosystems, ensuring that stakeholders are well-informed and equipped to implement effective security measures.

Furthermore, the research contributes to the aspect of network protocols in the broader discourse on IoT security by examining how different protocols impact the security posture of IoT devices, which brings attention to the interconnectedness of hardware, software, and communication frameworks in the IoT ecosystem. This holistic perspective enhances the understanding of the complicated relationship between IoT devices and the network protocols that facilitate their communication, leading to more informed decisions regarding security implementations and protocol selection. Finally, the research contributes by consolidating dispersed information on IoT security into a coherent and accessible resource by synthesizing existing knowledge to aid both newcomers and seasoned professionals in the field by providing a consolidated overview of the state of IoT device security and the role of network protocols. This not only facilitates a deeper understanding of the challenges but also encourages further research and innovation in the development of robust security measures for IoT devices.

After conducting a thorough survey on "IoT Device Security and Network Protocols," several promising avenues for future research emerged. Firstly, researchers may explore advanced cryptographic techniques tailored to the resource-constrained nature of many IoT devices. Developing lightweight yet robust encryption methods could significantly enhance the security of IoT networks, addressing the challenges posed by the limited computational capabilities of these devices. Secondly, there is a need for in-depth investigations into the human-centric aspects of IoT security. Understanding user behaviours, perceptions, and interactions with IoT devices can contribute to the design of more effective security measures. Human factors such as usability, privacy concerns, and user education play a fundamental role in the overall security of IoT systems, and future studies can delve into optimizing these elements for enhanced user awareness and engagement. Additionally, research efforts could focus on standardization and interoperability of security protocols within the IoT ecosystem. As the number and diversity of IoT devices continue to grow, ensuring seamless integration and communication between devices from different manufacturers becomes crucial. Future studies may explore the development of standardized security protocols that can be universally implemented, fostering a more secure and cohesive IoT environment. This could involve collaboration with industry stakeholders and standardization bodies to establish guidelines for secure IoT implementations, promoting a more robust and uniform security landscape.

V. CONCLUSION

In conclusion, this work has provided a comprehensive examination of the prevailing challenges, vulnerabilities, and countermeasures in the realm of IoT device security. The research meticulously identified and analyzed the multifaceted landscape of IoT security, emphasizing the critical role played by network protocols. The exploration of current challenges has underscored the complex nature of threats faced by IoT devices, ranging from unauthorized access to potential data breaches, highlighting the importance of robust security measures. Furthermore, the survey shed light on vulnerabilities that could compromise the integrity, confidentiality, and availability of data within IoT networks. The insights gained from this analysis are instrumental in understanding the nuanced security issues surrounding IoT devices, guiding researchers, practitioners, and policymakers toward more effective countermeasures. By delving into the intricacies of network protocols, the research contributes valuable knowledge to the ongoing discourse on fortifying the security posture of IoT ecosystems. Looking ahead, future research directions may involve the development of lightweight cryptographic techniques tailored to resource-constrained IoT devices, as well as a deeper exploration of human-centric aspects, such as user behaviours and perceptions, to optimize security measures. Standardization and interoperability of security protocols within the IoT ecosystem also emerge as crucial areas for further investigation to ensure a cohesive and universally secure IoT landscape. Overall, this survey serves as a foundational resource for advancing the understanding and implementation of effective security measures in the dynamic field of IoT device security and network protocols.

REFERENCES

[1] Mahmoud, C., & Aouag, S. (2019, March). Security for the Internet of things: A state of the art on existing protocols and open research issues. In *Proceedings of the 9th International Conference on Information Systems and Technologies* (pp. 1-6).

[2] Xu, T., Wendt, J. B., & Potkonjak, M. (2014, November). Security of IoT systems: Design challenges and opportunities. In *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)* (pp. 417-423). IEEE.

[3] Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends. *Wireless communications and mobile computing*, *2018*.

[4] Nebbione, G., & Calzarossa, M. C. (2020). Security of IoT application layer protocols: Challenges and findings. *Future Internet*, *12*(3), 55.

[5] Rahman, R. A., & Shah, B. (2016, March). Security analysis of IoT protocols: A focus in CoAP. In *2016 3rd MEC International Conference on Big Data and Smart Cities (ICBDSC)* (pp. 1-7). IEEE.

[6] Krejčí, R., Hujňák, O., & Švepeš, M. (2017, November). Security survey of the IoT wireless protocols. In *2017 25th Telecommunication Forum (TELFOR)* (pp. 1-4). IEEE.

[7] Hеđi, I., Špeh, I., & Šarabok, A. (2017, May). IoT network protocols comparison for the purpose of IoT-constrained networks. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 501-505). IEEE.

[8] Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications*, *169*, 102763.

[9] Gupta, B. B., & Quamara, M. (2020). An overview of the Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience*, *32*(21), e4946.

[10] Aksoy, A., & Gunes, M. H. (2019, May). Automated IoT device identification using network traffic. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

[11] Tournier, J., Lesueur, F., Le Mouël, F., Guyon, L., & Ben-Hassine, H. (2021). A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things*, *16*, 100264.

DOI: 10.17148/IARJSET.2024.11701

[12] Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2017, October). A lightweight IoT security protocol. In *2017 1st cyber security in networking conference (CSNet)* (pp. 1-8). IEEE.

[13] Dragomir, D., Gheorghe, L., Costea, S., & Radovici, A. (2016, September). A survey on secure communication protocols for IoT systems. In *2016 international workshop on Secure Internet of Things (IoT)* (pp. 47-62). IEEE.

[14] Sardeshmukh, H., & Ambawade, D. (2017, June). Internet of Things: Existing protocols and technological challenges in security. In *2017 International Conference on Intelligent Computing and Control (I2C2)* (pp. 1-7). IEEE.

[15] Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for the Internet of Things. *Future Generation Computer Systems*, *89*, 110-125.

[16] Cynthia, J., Parveen Sultana, H., Saroja, M. N., & Senthil, J. (2019). Security protocols for IoT. *Ubiquitous computing and computing security of IoT*, 1-28.

[17] Gope, P., & Sikdar, B. (2018). Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet of Things Journal*, *6*(1), 580-589.

[18] Thilakarathne, N. N., Samarasinghe, R., Dasanayake, D. M. C. K., Fasla, M. F. F., Ananda, A. M. S. D., Sonnadara, G. H., ... & Silva, D. S. D. (2022). Internet of Things (IoT) Security: Status, Challenges and Countermeasures. *International Journal of Advanced Networking and Applications*, *14*(3), 5444-5454.

[19] Moran, B., Tschofenig, H., Brown, D., & Meriac, M. (2021). A firmware update architecture for the Internet of Things. *draft-ietf-suit-architecture-08*.

[20] Aftab, M. U., Oluwasanmi, A., Alharbi, A., Sohaib, O., Nie, X., Qin, Z., & Ngo, S. T. (2021). Secure and dynamic access control for the Internet of Things (IoT) based traffic system. *PeerJ Computer Science*, *7*, e471.

[21] Zamfir, S., Balan, T., Iliescu, I., & Sandu, F. (2016, October). A security analysis on standard IoT protocols. In *2016 international conference on applied and theoretical electricity (ICATE)* (pp. 1-6). IEEE.

[22] Ahmet, E. F. E., Aksöz, E., Hanecioğlu, N., & Yalman, Ş. N. (2018). Smart security of IoT against DDoS attacks. *International Journal of Innovative Engineering Applications*, *2*(2), 35-43.

[23] Yang, X., Shu, L., Liu, Y., Hancke, G. P., Ferrag, M. A., & Huang, K. (2022). Physical security and safety of IoT equipment: A survey of recent advances and opportunities. *IEEE Transactions on Industrial Informatics*, *18*(7), 4319-4330.

[24] Jahangeer, A., Bazai, S. U., Aslam, S., Marjan, S., Anas, M., & Hashemi, S. H. (2023). A Review on the Security of IoT Networks: From Network Layer's Perspective. *IEEE Access*.

[25] Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., ... & Ghorbani, A. A. (2023). Internet of Things (IoT) security dataset evolution: Challenges and future directions. *Internet of Things*, 100780.

[26] Khan, N. A., Awang, A., & Karim, S. A. A. (2022). Security in Internet of Things: A review. *IEEE Access*, *10*, 104649-104670.

[27] Kasif, A., Togay, C., & Levi, A. (2021, September). Securing Internet of Things networks with gateways and multi-SSID technology. In *2021 International Balkan Conference on Communications and Networking (BalkanCom)* (pp. 45-50). IEEE.

[28] Pahlevi, R. R., Suryani, V., Nuha, H. H., & Yasirandi, R. (2022, August). Secure two-factor authentication for IoT devices. In *2022 10th International Conference on Information and Communication Technology (ICoICT)* (pp. 407-412). IEEE.

[29] Kumar, R., Singh, S., Singh, D., Kumar, M., & Gill, S. S. (2024). A robust and secure user authentication scheme based on multifactor and multi-gateway in IoT-enabled sensor networks. *Security and Privacy*, *7*(1), e335.

[30] Hussain, I. (2024). Secure, Sustainable Smart Cities and the Internet of Things: Perspectives, Challenges, and Future Directions. *Sustainability*, *16*(4), 1390.

[31] Ullah, I., Noor, A., Nazir, S., Ali, F., Ghadi, Y. Y., & Aslam, N. (2024). Protecting IoT devices from security attacks using an effective decision-making strategy of appropriate features. *The Journal of Supercomputing*, *80*(5), 5870-5899.

[32] Hubert, K., & Kaledio, P. (2024). Security and Privacy in IoT: Considerations for securing IoT devices.

[33] Singh, I., & Singh, B. (2023). Access management of IoT devices using access control mechanism and decentralized authentication: A review. *Measurement: Sensors*, *25*, 100591.

[34] Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in the Internet of things: Challenges, countermeasures, and future directions. *Ad Hoc Networks*, 103159.

[35] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. *IEEE Access*.

[36] Ahmed, S., & Khan, M. (2023). Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem. *AI, IoT and the Fourth Industrial Revolution Review*, *13*(9), 1-17.

[37] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

[38] Rozlomii, I., Yarmilko, A., & Naumenko, S. (2024, April). Data security of IoT devices with limited resources: challenges and potential solutions. In *Proceedings of the 4th Edge Computing Workshop (doors 2024), Zhytomyr, Ukraine* (pp. 85-96).

[39] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. *IEEE Access*.

[40] Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors*, *24*(2), 708.

[41] Bhardwaj, A., Kaushik, K., Alshehri, M., Mohamed, A. A. B., & Keshta, I. (2023). ISF: Security analysis and assessment of smart home IoT-based firmware. *ACM Transactions on Sensor Networks*.

[42] Ul Haq, S., Singh, Y., Sharma, A., Gupta, R., & Gupta, D. (2023). A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks. *Discover Internet of Things*, *3*(1), 17.

[43] El Jaouhari, S., & Bouvet, E. (2022). Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions. *Internet of Things*, *18*, 100508.

[44] Hernández-Ramos, J. L., Baldini, G., Matheu, S. N., & Skarmeta, A. (2020, June). Updating IoT devices: challenges and potential approaches. In *2020 Global Internet of Things Summit (GIoTS)* (pp. 1-5). IEEE.

[45] Arakadakis, K., Charalampidis, P., Makrogiannakis, A., & Fragkiadakis, A. (2021). Firmware over-the-air programming techniques for IoT networks-A survey. *ACM Computing Surveys (CSUR)*, *54*(9), 1-36.

[46] Wang, J., Zhu, M., Li, M., Sun, Y., & Tian, Z. (2023). An access control method against unauthorized and non-compliant behaviors of real-time data in industrial IoT. *IEEE Internet of Things Journal*.

[47] Khalid, M., Hameed, S., Qadir, A., Shah, S. A., & Draheim, D. (2023). Towards SDN-based smart contract solution for IoT access control. *Computer Communications*, *198*, 1-31.

[48] Ragothaman, K., Wang, Y., Rimal, B., & Lawrence, M. (2023). Access control for IoT: A survey of existing research, dynamic policies, and future directions. *Sensors*, *23*(4), 1805.

[49] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. *IEEE Access*.

[50] Kizza, J. M. (2024). Access control and authorization. In *Guide to Computer Network Security* (pp. 195-214). Cham: Springer International Publishing.

[51] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. *IEEE Access*.

[52] Almarri, S., & Frikha, M. (2024). Authentication and Access Control Mechanisms to Secure IoT Environments: A comprehensive SLR.

[53] Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications*, *169*, 102763.

[54] Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IoT: a survey. *Wireless Personal Communications*, *115*(2), 1667-1693.

[55] Rachit, Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. *SN Applied Sciences*, *3*, 1-14.

[56] Nzeako, G., Okeke, C. D., Akinsanya, M. O., Popoola, O. A., & Chukwurah, E. G. (2024). Security paradigms for IoT in telecom networks: Conceptual challenges and solution pathways. *Engineering Science & Technology Journal*, *5*(5), 1606-1626.

[57] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. *IEEE Access*.

[58] Bhoi, S. K., Ghugar, U., Dash, S., Nayak, R., & Bagal, D. K. (2024). Exploring The Security Landscape: A Comprehensive Analysis Of Vulnerabilities, Challenges, And Findings In Internet Of Things (IoT) Application Layer Protocols. *Migration Letters*, *21*(S6), 1326-1342.

[59] Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Security and Privacy*, *6*(6), e318.

[60] Bakhsh, S. A., Khan, M. A., Ahmed, F., Alshehri, M. S., Ali, H., & Ahmad, J. (2023). Enhancing IoT network security through deep learning-powered Intrusion Detection System. *Internet of Things*, *24*, 100936.

[61] Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*, *26*(6), 3753-3780.

[62] Farooq, M., Khan, M. H., & Khan, R. A. (2023). Implementation of Network Security for Intrusion Detection & Prevention System in IoT Networks: Challenges & Approach. *Int. J. Advanced Networking and Applications*, *15*(05), 6109-6113.

[63] Alazab, M., Awajan, A., Alazzam, H., Wedyan, M., Alshawi, B., & Alturki, R. (2024). A Novel IDS with a Dynamic Access Control Algorithm to Detect and Defend Intrusion at IoT Nodes. *Sensors*, *24*(7), 2188.

[64] Samita. (2024). A Review on Intrusion Detection System for IoT-based Systems. *SN Computer Science*, *5*(4), 380.

[65] Fatima, M., Rehman, O., Ali, S., & Niazi, M. F. (2024). ELIDS: Ensemble Feature Selection for Lightweight IDS against DDoS attacks in a resource-constrained IoT environment. *Future Generation Computer Systems*.

[66] Mahanta, K., & Maringanti, H. B. Security in the Internet of Things (IoT): Developing intrusion detection systems for IoT devices and networks and addressing the unique security challenges posed by this connected environment.

[67] Taherdoost, H. (2023). Security and internet of things: benefits, challenges, and future perspectives. *Electronics*, *12*(8), 1901.

[68] Siwakoti, Y. R., Bhurtel, M., Rawat, D. B., Oest, A., & Johnson, R. C. (2023). Advances in IOT security: Vulnerabilities, enabled Criminal Services, attacks and countermeasures. *IEEE Internet of Things Journal*.

[69] Ahmid, M., & Kazar, O. (2023). A comprehensive review of the Internet of Things security. *Journal of Applied Security Research*, *18*(3), 289-305.

[70] Arnold, R. C. (2023). *Internet of Things (IoT) devices and security: A narrative review* (Doctoral dissertation, Georgia State University).

[71] Vetrivel, S. C., Maheswari, R., & Saravanan, T. P. (2024). Industrial IoT: Security Threats and Counter Measures. In *Communication Technologies and Security Challenges in IoT: Present and Future* (pp. 403-425). Singapore: Springer Nature Singapore.

[72] Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). IoT vulnerabilities and attacks: SILEX malware case study. *Symmetry*, *15*(11), 1978.

[73] Vetrivel, S. C., Maheswari, R., & Saravanan, T. P. (2024). Industrial IoT: Security Threats and Counter Measures. In *Communication Technologies and Security Challenges in IoT: Present and Future* (pp. 403-425). Singapore: Springer Nature Singapore.

[74] Babu, C. S., Pal, A., Vinith, A., Muralirajan, V., & Gunasekaran, S. (2024). Enhancing cloud and IOT security: Leveraging IOT technology for multi-factor user authentication. In *Emerging Technologies for Securing the Cloud and IoT* (pp. 258-282). IGI Global.

[75] Mughaid, A., Obeidat, I., Abualigah, L., Alzubi, S., Daoud, M. S., & Migdady, H. (2024). Intelligent cybersecurity approach for data protection in cloud computing based internet of things. *International Journal of Information Security*, 1-15.

[76] Goel, A., & Sahil, G. (2023). Implementing privacy and data confidentiality within the framework of the Internet of Things. *Journal of Data Protection & Privacy*, *5*(4), 374-387.

[77] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the Internet of Healthcare Things (IoHTs). *Applied Sciences*, *12*(4), 1927.

[78] Politou, E., Alepis, E., Virvou, M., & Patsakis, C. (2022). *Privacy and data protection challenges in the distributed era* (Vol. 26, pp. 1-185). Heidelberg, Germany: Springer.

[79] Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review*, *38*, 100312.

[80] Cottrill, C. D., Jacobs, N., Markovic, M., & Edwards, P. (2020). Sensing the city: designing for privacy and trust in the internet of things. *Sustainable Cities and Society*, *63*, 102453.

[81] Dhasaratha, C., Hasan, M. K., Islam, S., Khapre, S., Abdullah, S., Ghazal, T. M., ... & Akhtaruzzaman, M. (2024). Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things. *CAAI Transactions on Intelligence Technology*.

[82] Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions, and recommendations. *Internet of Things and Cyber-Physical Systems*, *3*, 280-308.

[83] Goeman, V., de Ruck, D., Bohé, I., Lapon, J., & Naessens, V. (2023, August). IoT Security Seminar: Raising Awareness and Sharing Critical Knowledge. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-8).

[84] Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). IoT vulnerabilities and attacks: SILEX malware case study. *Symmetry*, *15*(11), 1978.

[85] Sallam, K., Mohamed, M., & Mohamed, A. W. (2023). Internet of Things (IoT) in supply chain management: challenges, opportunities, and best practices. *Sustainable Machine Intelligence Journal*, *2*, 3-1.

[86] Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in the Internet of things: Challenges, countermeasures, and future directions. *Ad Hoc Networks*, 103159.

[87] Tariq, U., Ahmed, I., Khan, M. A., & Bashir, A. K. (2023). Fortifying IoT against crimpling cyber-attacks: a systematic review. *Karbala International Journal of Modern Science*, *9*(4), 9.

[88] Taherdoost, H. (2023). Security and internet of things: benefits, challenges, and future perspectives. *Electronics*, *12*(8), 1901.

[89] Devan, K. P. K., Liya, B. S., & Indumathy, P. (2024). Security and Privacy Issues in IoT. In *Secure Communication in Internet of Things* (pp. 266-278). CRC Press.

[90] Ahmadi, S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. *Journal of Engineering Research and Reports*, *26*(2), 215-228.

DOI: 10.17148/IARJSET.2024.11701

[91] Zaki, H. (2024). *Addressing IoT Security: Understanding Challenges, Threats, and Countermeasures* (No. 12019). EasyChair.

[92] Babu, C. S., Pal, A., Vinith, A., Muralirajan, V., & Gunasekaran, S. (2024). Enhancing cloud and IOT security: Leveraging IOT technology for multi-factor user authentication. In *Emerging Technologies for Securing the Cloud and IoT* (pp. 258-282). IGI Global.

[93] Hussain, A., Hussain, A., Qadri, S., Razzaq, A., Nazir, H., & Ullah, M. S. (2024). Enhancing LAN Security by Mitigating Credential Threats via HTTP Packet Analysis with Wireshark. *Journal of Computing & Biomedical Informatics*, *6*(02), 433-440.

[94] Ali, S., Li, Q., & Yousafzai, A. (2024). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey. *Ad Hoc Networks*, *152*, 103320.

[95] Omotunde, H., & Ahmed, M. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. *Mesopotamian Journal of CyberSecurity*, *2023*, 115-133.

[96] Ragothaman, K., Wang, Y., Rimal, B., & Lawrence, M. (2023). Access control for IoT: A survey of existing research, dynamic policies, and future directions. *Sensors*, *23*(4), 1805.

[97] Kallatsa, M. (2024). Strategies for network segmentation: a systematic literature review.