Securing the Industrial IoT: A Comprehensive Review of Security Challenges and Emerging Solutions

Mohd Abdullah, Dr. Jawed Ahmed
Jamia Hamdard, Department of Computer Science & Engineering, School of Engineering Sciences & Technology, New Delhi, INDIA-110062
Mohd.abdullah9707@gmail.com; Jawed2047@gmail.com

***Abstract*—** By facilitating automation, predictive analytics, and smarter operations, IIoT is transforming industries. However, it also presents cybersecurity issues that need to be resolved with strong standards, cutting-edge security solutions, and AI-powered threat detection. Secure, effective, and scalable solutions that boost industrial efficiency while guaranteeing data protection are the key to the IIoT's future. This study highlights how the amalgamation of physical processes with digital systems facilitates industrial automation and self-management across di-verse systems, including smart factories, autonomous cars, and robotic process automation. The study tries to do thematic analysis and based on those themes the study aims to identify cybersecurity threats, assess their impact on industries like manufacturing, energy, healthcare, and logistics, explore advancements in cyber-security, examine existing standards, and understand regulatory policies' role in IIoT network security and analyse the recommended solutions. The study finally finds out that IIoT network cyberattacks create several protection risks that generate industrial production disturbance while endangering financial stability and leading to data breaches along with risking permanent damage to industrial equipment. Security protection of IIoT devices and networks and their related da-ta remains a complex challenge even when industries need to maintain their operational standards.

***Keywords*—** *Cybersecurity, IIOT, Zero-trust Network)*

I. INTRODUCTION

A. Overview of the research topic and its importance

The Industrial Internet of Things (IIoT) is revolutionising industries by enabling real-time data acquisition, automation, and enhanced operational efficiency. The Indus-trial Internet of Things (IIoT) improves productivity and decision-making through the integration of equipment, sensors, and systems across industries including manufacturing, energy, healthcare, and logistics. However, the increased connectivity of IIoT systems creates substantial cybersecurity vulnerabilities that makes them vulnerable to cyberattacks [1]. The network topology of IIoT differs significantly from typical IT infrastructure since it contains multiple legacy systems and essential infrastructure together with remote industrial assets that normally operate without security measures. The research analyzes primary security risks affecting the Industrial Inter-net of Things (IIoT) which arises from network weaknesses as well as targeted device attacks and the vulnerability of data materials [2]. The paper evaluates future security solutions by studying AI threat detection along with blockchain-based security and zero-trust networks and quantum encryption which serve to protect industrial operations. Organisations will achieve enhanced security alongside business continuity protection and vital asset safety by addressing these matters during the IIoT era.

B. Key Concepts and Scope

IIoT functions as an industrial technology that enables linked sensors and devices to transmit operational data instantly through industrial national networks. Processing data at the edge through local computing systems near its origins produces fast reaction times and improved security features based on this method [3]. Operational in-formation analysis by IIoT depends on both cloud computing and big data analytics as well as artificial intelligence and machine learning systems for predictive repairs and process defect recognition alongside optimization tasks. The researchers will perform assessments regarding cybersecurity threats alongside their sectoral effects on manufacturing and energy along with healthcare and logistics alongside a review of security modernization and investigation of IIoT network security regulatory policies.

C. Objectives of the review and the research question(s).

Objective

- To identify the primary cybersecurity threats, including data breaches, unauthorized access, and network vulnerabilities.
- To assess how security vulnerabilities affect operational efficiency, business continuity, and financial losses in industries such as manufacturing, energy, healthcare, and logistics.
- To investigate the latest advancements in cybersecurity, such as AI-driven threat detection, blockchain security, zero-trust architecture, and secure communication protocols.
- To examine existing security standards (e.g., IEC 62443, NIST Cybersecurity Framework) and their role in protecting IIoT infrastructures.
- To understand the role of regulatory policies in securing IIoT networks while recommending practical solutions to mitigate the issues.

Research Question.

- What are the primary cybersecurity threats, including data breaches, unauthorized access, and network vulnerabilities?
- How security vulnerabilities affect operational efficiency, business continuity, and financial losses in industries such as manufacturing, energy, healthcare, and logistics?

- What are the latest advancements in cybersecurity, such as AI-driven threat detection, blockchain security, zero-trust architecture, and secure communication protocols?
- What are the existing security standards and their role in protecting IIoT infra-structures?
- What is the role of regulatory policies in securing IIoT networks while recommending practical solutions to mitigate the issues?

II. LITERATURE REVIEW

A. *Thematic Analysis*

1) Security of the internet of things: Challenges and Opportunities

"Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications": The Internet of Things (IoT) presents multiple development possibilities to manufacturers and industrial applications that aim to build smart grids and cities. Protection against hacking attempts remains a necessary reality for IoT systems because of its susceptibility to attacks therefore organizations must implement diverse protective security measures to stay secure. Security dangers become more severe when IIoT technology finds wide acceptance. The analysis investigates industrial IoT system integrity that includes current security protocols for significant industrial applications. Multiple sections present the content of the research by describing IoT attacks while discussing security solutions for IoT layers and performing an evaluation of existing research related security measures and IoT/IIoT solutions with different security methods [4]. An extended discussion about IoT/IIoT security research challenges appears in this study after performing a survey about such matters. Results demonstrate that IoT technology provides sensors and control systems with physical connectivity and computing capability together with automatic data creation and exchange capabilities. Embedded security vulnerabilities can be found across the IoT system at both network, middleware, communication protocol and application layers.

"Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, se-curity issues and blockchain solutions for IoT and IIoT": The development of automation systems at home and in industry finds its roots in the critical Internet of Things (IoT) opportunity that leads to Industrial Internet of Things (IIoT). The cyberattack vulnerability of IoT systems creates difficulties for security because it requires different security solutions. The industrial implementation of IIoT technological systems leads to increased security threats throughout manufacturing facilities. The study introduces an attack classification method based on vulnerability object evaluation and illustrates its relationship with general IoT/IIoT architecture components and includes examples of documented countermeasures and real-life attacks from the literature [5]. Research demonstrates security protection approaches for IIoT threats alongside descriptions of core applications involved in industrial IoT deployments. Blockchain technology offers an appropriate solution to handle the multiple issues stemming from centralized IoT/IIoT infrastructure. This study exam-ines the Tangle design made for IoT blockchain systems and the best blockchain solution that can function as an alternative to traditional cloud application management. The paper explores security research domains of IoT/IIoT before presenting targeted solutions for each research area. The research should dedicate future investigations to the selected open research domains. This study reaches a final conclusion about Internet of Things (IoT) since it leads to increased security risks including de-vice infiltrations and data breaches while in transit. The development of IIoT re-search led to its emergence as an independent field because smart systems brought accelerated integration between physical and virtual domains.

2) Latest advancements in cybersecurity and the solutions being implemented.

"Tan, S.F. and Samsudin, A., (2021). Recent technologies, security countermeasures and ongoing challenges of Industrial Internet of Things (IIoT): A survey.": Multiple surveys have investigated these matters yet existing research fails to bridge the security requirement gap with actual field-implemented countermeasures in industrial settings. A detailed survey of IIoT security examines the four-layer architecture together with respective countermeasures which support CIA+ security requirements and the evaluation of existing countermeasures weaknesses [6]. The article argues for a data-oriented solution to overcome industrial deployment challenges through data protection coverage at all locations while using a bottom-up methodology with in-creased abstraction levels to address ecosystem complexities. The IIoT security architecture, along with related industry technologies and standards, are thoroughly examined in this article. This article began by going over the definitions and features of the IIoT and highlighting the security issues that are unique to the IIoT and not related to the data security issues that are currently in place. The study then suggested a new four-layer IIoT security design after reviewing existing IIoT architectures. The suggested security architecture is built using a bottom-up methodology. Every layer of the suggested IIoT architecture undergoes a thorough end-to-end security review. This involves discussing current security issues and upcoming projects, highlighting their recent industry counter measurements and shortcomings, and evaluating security requirements using the CIA+ model.

"Gebremichael, T., Ledwaba, L. P., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and privacy in the industrial internet of things: The Industrial IoT (IIoT) functions as an accelerated segment of industrial markets because it provides contemporary business frameworks and analytical soft-ware and open-source decision-making tools. IIoT deployments exist at risk of security threats due to their infrastructure presenting significant complexity challenges. Three major consequences from IIoT infrastructure security threats produce network operation distrust as well as crucial infrastructure loss and breach end-user security through privacy violations of sensitive data. This paper examines IIC and OpenFog Consortium security standards to assess current IIoT connectivity standards and their features for privacy and security. This research examines upcoming research

possibilities that target greater security in addition to privacy and safety features of the IIoT. Writing from the study states that The Internet of Things (IoT) shapes industrial transformation through modern methods of factory management as well as vital safety system control procedures [7]. The IIoT presents challenges for security and privacy protection because its intricate nature makes specification of explicit security requirements difficult to implement.

3) Existing security standards and their compliance in IIOT alongside mitigation strategies.

"Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments.": An examination of IoT-based smart environment security frameworks and standardizations according to Karie et al. (2021) was conducted in this paper." This paper analysis indicates that a review of existing security standards and assessment frameworks investigates this shortcoming. NIST special publications provide security techniques with main points of emphasis to identify which solutions will meet the security requirements of IoT based smart environments. A study analyzed 37 assessment frameworks for conventional security which included 7 security procedure documents from NIST special publications alongside 80 security standards from ISO/IEC and 32 standards from ETSI. To reflect the latest research findings, the assessment approach used existing security standards, evaluation systems and developmental activities. Although most established security standards and evaluation systems are compatible with IoT based smart environments, they often fail to address specific security demands. The research project supports IoT progress through developing different pathways for security standards and evaluation frameworks that tackle future security risks in IoT-enabled smart environments [8]. This research delivers information about present-day security standards and evaluation frameworks through its state-of-the-art research design description. Security challenges find their solutions through this document.

4) Ethical Considerations in IIOT

"Marinova, N. (2024). Advantages and Ethical Considerations of Industrial IoT Artificial Intelligence Solutions Usage. Бизнес управление, (2), 43-58": The purpose of this paper is to analyze the interdependent relationship between implementing artificial intelligence (AI) in IIoT ecosystems in conjunction with Industrial Inter-net of Things (IIoT). The research adopts an integrative study approach which com-bines essential academic literature about "Industrial Internet of Things" and "Artificial Internet of Things" and utilises the PRISMA flow chart to construct the document list. A content analysis approach became essential for different subject groups because the detailed study of the AIoT issue required more than one article could provide. Most recent scholarly work focused on the IIoT and AIoT ideas with various theoretical and practical approaches since the beginning of the prior five years [9]. The manuscript establishes its novelty through its systematic exploration of dominant characteristics as well as advantages and risks in present-day applications such as self-driving vehicles and robotics and intelligent machinery for production along-side preventive maintenance and descriptions of green and eco-friendly AIoT possibilities. Partners in AIoT need to consider all necessary risks along with ethical factors before deployment because this assessment defines how businesses positively impact society.

III. CRITICAL ANALYSIS

TABLE I COMPARISON OF ARTICLES

Methodologies	Strengths	Research Gaps	Study Name
Uses survey method which will provide the blueprint for security improvement in IoT industrial use cases.	It critically evaluates current IoT solutions based on cryptography and IDSs, and formulates future directions for research with a view to improving security levels.	Addresses the security and challenges of IIOT.	"Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications."
Uses survey method. The survey emphasizes the importance of addressing the emerging threats proactively and building strong security solutions based on blockchain technologies.	The paper establishes security research areas for IoT/IIoT and details appropriate solutions within each area. Future investigation should focus on the selected open research domains.	Addresses the security and challenges of IIOT.	"Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT."
This study utilised a survey method to identify the latest advancement in IIOT and countermeasures that are applicable to solve potential issues.	This involves discussing current security issues and upcoming projects, highlighting their recent industry counter measurements and shortcomings, and evaluating security requirements using the CIA+ model.	Addresses latest advancements in cybersecurity and the solutions being Implemented.	"Tan, S.F. and Samsudin, A., 2021. Recent technologies, security countermeasures and ongoing challenges of Industrial Internet of Things (IIoT): A survey."
The paper follows review method where security standards from IIC and OpenFog	The current paper offers a complete picture of security and privacy in the IIoT,	Addresses Latest advancements in cybersecurity and the	Gebremichael, T., Ledwaba, L. P., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J.

Consortium is looked upon to analyze current IIoT connectivity protocols alongside their privacy and security aspects.	examining multiple protocols and solutions, identifying security vulnerabilities and weaknesses.	solutions being Implemented.	(2020). Security and privacy in the industrial internet of things: Current standards and future challenges."
Research covered 37 conventional security assessment frameworks consisting of 7 NIST special publications on security procedures and 80 ISO/IEC security standards and 32 ETSI standards.	This research creates a classification of IoT-based smart environment security problems after analyzing the extensive literature available. The document connects security problems with potential answers.	Works on existing security standards and their compliance in IIOT alongside mitigation strategies.	Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environment.
Uses Literature Review method. Investigated from diverse theoretical and practical perspectives in many studies, primarily within the past five years.	This paper aims to explore the symbiotic relationship between the use of artificial intelligence (AI) in IIoT ecosystems and the Industrial Internet of Things (IIoT).	Focuses on Ethical Considerations in IIOT.	Marinova, N. (2024). Advantages and Ethical Considerations of Industrial IoT Artificial Intelligence Solutions Usage. Бизнес управление, (2), 43-58"

IV. RECENT DEVELOPMENTS

The main driver behind Industry 4.0 functions through sensors that deliver real-time data needed to monitor operations remotely. The accuracy of these systems gets an enhancement through the implementation of machine learning technology [10]. The implementation of 5G networking technology together with sensor advances enables facilities to install more sensors gathering a greater amount of data thereby enhancing their understanding of data points.

The implementation of 5G alongside edge computing technologies will enhance the IIoT infrastructure because industrial edge computing enables machines to exchange data with central servers and yield performance-based insights. Fog computing makes intelligent networks relocate their capabilities to near-network areas where they offer real-time performance improvements along with better security and enhanced administration. Through IoT technology organizations can track their staff and their contacts as well as log body temperatures for individualized safety measures [11]. The IoT enables manufacturers to respond quickly to their supplier selections and procurement strategies and their ordering protocols. Systems require quantum-resistant encryption technologies for protection because hackers now have more attack avenues through which they operate.

AI integration with machine learning algorithms already appears in mainstream applications whereas these platforms enable IIoT systems to make predictive maintenance predictions and acknowledge anomalies as well as deliver automated decision outcomes. The development of human-machine systems together with virtual reality and augmented reality technology will become standardized throughout our work environment. By 2025 AI assistants will establish a wider presence so people can communicate effectively with machines. The implementation of IIoT in manufacturing operations will generate substantial positive effects through the foreseeable future [12]. Within the IIoT environment standardization plays a crucial role since it handles device operational security requirements. Almost all standards fail to provide detailed instructions to reach their intended outcomes. The standards divide between those handling data exchange protocols and communication standards and the other security-focused standards such as ISO/IEC 27017 and ENISA and C-SIG which concentrate on cloud platform operational security [13]. Current assessment findings indicate the lack of a unified security standard which covers every stage of the IIoT framework starting from devices and reaching to backend platforms. Multiple measurable security safety and organizational metrics originating from different standards need to be combined to build complete system coverage. A metric model serves as a solution for this problem and will be demonstrated in the following section.

V. CONCLUSION

A. Summary of Key Insights

Within the scope of the study, real-time equipment monitoring and predictive failure predictions that occur through this technology help decrease costs connected to downtime alongside maintenance requirements is addressed. Hacking, data breaches, and ransomware incidents are among the safety threats associated with IIoT attacks; however, organisations address these issues by implementing zero-trust architectures, end-to-end encryption systems, and AI-powered threat identification techniques.

B. Research Gaps

The current security standards for IIoT environments prove insufficient because they are generic and designed for environments that are less complex [10]. New methodologies should combine IIoT related security vulnerabilities with automatic threat handling procedures. The research of AI-driven cybersecurity for IIoT remains underdeveloped because analysts need to study its effectiveness in industrial networks to detect zero-day attacks. Security approaches tend to focus their effort on post-attack mitigation instead of focusing on real-time threat detection and response methods. At the same time there is a lack of attention on real-time threat detection and response.

VI. SUGGESTED DIRECTIONS FOR FUTURE RESEARCH

Industry Internet of Things equipment utilizing edge and cloud processing modes faces high risks during information transmission as well as information processing operations. Scientists need to develop new encryption protocols and

blockchain-based security systems for ensuring secure cloud-edge integration. The fast industrial implementation of 5G-enabled IIoT brings security problems that demand new research on 5G security protocols suitable for industrial environments. Future investigations must focus on all these elements for proper development.

REFERENCES

[1]. Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: Challenges and solutions. Wireless Personal Communications, 119, 2603-2637.

[2]. Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors, 21(11), 3654.

[3]. Alnajim, A. M., Habib, S., Islam, M., Thwin, S. M., & Alotaibi, F. (2023). A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in industrial internet of things. Technologies, 11(6), 161.

[4]. Bicaku, A., Tauber, M., & Delsing, J. (2020). Security standard compliance and continuous verification for Industrial Internet of Things. International Journal of Distributed Sensor Networks, 16(6), 1550147720922731.

[5]. Borgiani, V., Moratori, P., Kazienko, J. F., Tubino, E. R., & Quincozes, S. E. (2020). Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial internet of things. IEEE Internet of Things Journal, 8(6), 4569-4578.

[6]. Gebremichael, T., Ledwaba, L. P., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and privacy in the industrial internet of things: Current standards and future challenges. IEEE Access, 8, 152351-152366.

[7]. Jayalaxmi, P., Saha, R., Kumar, G., Kumar, N., & Kim, T. H. (2021). A taxonomy of security issues in Industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges. IEEE Access, 9, 25344-25359.

[8]. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEe Access, 9, 121975-121995.

[9]. Marinova, N. (2024). Advantages and Ethical Considerations of Industrial IoT Artificial Intelligence Solutions Usage. Бизнес управление, (2), 43-58.

[10]. Mirani, A. A., Velasco-Hernandez, G., Awasthi, A., & Walsh, J. (2022). Key challenges and emerging technologies in industrial IoT architectures: A review. Sensors, 22(15), 5836.

[11]. Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of network and computer applications, 149, 102481.

[12]. Serror, M., Hack, S., Henze, M., Schuba, M., & Wehrle, K. (2020). Challenges and opportunities in securing the industrial internet of things. IEEE Transactions on Industrial Informatics, 17(5), 2985-2996.

[13]. Tan, S.F. and Samsudin, A., 2021. Recent technologies, security countermeasure and ongoing challenges of Industrial Internet of Things (IIoT): A survey. Sensors, 21(19), p.6647.

Mohd Abdullah is a student of M.Tech (CSE). (Final Year) in Computer Science & Engineering at Jamia Hamdard, New Delhi. Abdullah has academic interests in the field of Cloud Computing, Cyber Security, Artificial Intelligence / Machine Learning, IOT etc.

Dr. Jawed Ahmed is an Assistant Professor at Jamia Hamdard, New Delhi. His research interests include Data Science, Bioinformatics, Big data analytics, and Machine Learning.