QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

ENHANCING IOT SECURITY THROUGH WIRELESS SENSOR NETWORKS

[1]Syeda Aqsa Zahra
Department of Computer Science, Superior University, Lahore, Pakistan
Email: Syedazahra208@yahoo.com
[2]Muhammad Mahtab
Department of Computer Science, Superior University, Lahore, Pakistan
[3]Syed Asad Ali Naqvi
Department of Information Technology, Superior University, Lahore, Pakistan
[4]Sadia Sahar
Department of Computer Science, Superior University, Lahore, Pakistan

Abstract:
The exponential growth of the Internet of Things (IoT) has introduced a wide array of security challenges, particularly in environments reliant on Wireless Sensor Networks (WSNs). As WSNs enable real-time data collection and monitoring, they become critical nodes in the IoT ecosystem but also introduce unique vulnerabilities. This paper explores these security challenges, focusing on weak authentication, data interception, and physical device tampering. It evaluates the role of intrusion detection systems (IDS), layered security protocols, and privacy-preserving techniques such as encryption and anonymization. Case studies using machine learning-based intrusion detection methods, including Particle Swarm Optimization (PSO) with Artificial Neural Networks (ANN), demonstrate high accuracy in threat identification. Furthermore, the integration of artificial intelligence, blockchain, and Zero Trust Architectures is proposed to reinforce the security posture of future IoT systems. The findings emphasize the necessity of adaptive and layered security strategies to safeguard sensitive data, ensure network resilience, and maintain public trust in increasingly connected environments.

Keywords: *Internet of Things (IoT), Wireless Sensor Networks (WSNs), Cybersecurity, Intrusion Detection Systems (IDS), Data Privacy, Machine Learning, Particle Swarm Optimization (PSO), Blockchain, Encryption, Zero Trust Architecture, Secure Communication Protocols, Anomaly Detection*

Introduction:

Enhancing IoT Security through Wireless Sensor Networks is a critical area of research and development aimed at addressing the significant security challenges posed by the rapidly growing Internet of Things (IoT) ecosystem. As IoT devices proliferate across sectors such as healthcare, transportation, and smart cities, their vulnerabilities have become increasingly evident, leading to a rise in cyber threats that can compromise sensitive data and operational integrity [1]. The integration of Wireless Sensor Networks (WSNs) plays a pivotal role in this landscape, enabling real-time data collection and monitoring while simultaneously introducing unique security concerns that must be effectively managed [2-4]. The notability of this topic stems from the increasing reliance on IoT systems, where security breaches can have severe implications, including data theft, unauthorized access, and threats to public safety [5]. Reports indicate that a significant number of IoT devices, particularly in healthcare [6], operate on outdated software with known vulnerabilities [7], making them prime targets for attacks [8]. Therefore, enhancing security

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

measures within WSNs is essential not only for safeguarding sensitive information but also for ensuring the reliability of critical services[9].

Prominent controversies in this field revolve around the balance between functionality and security[10], as implementing robust protective measures can sometimes impede the performance and usability of IoT systems. For instance, weak authentication methods and inadequate data encryption are common challenges that facilitate unauthorized access and data interception, leading to calls for improved security frameworks and best practices[11]. As technologies such as artificial intelligence[12-14] and blockchain[15] begin to integrate into IoT security strategies, the potential for enhanced resilience against emerging cyber threats is promising but also raises new concerns regarding privacy and complexity in implementation[16-18].

Table 1: Comparison of Security Protocols in WSNs

Protocol	Encryption Type	Lightweight	Suitable for IoT?	Vulnerabilities Addressed
AES	Symmetric	Medium	Yes	Data integrity, confidentiality
ECC	Asymmetric	High	Yes	Secure key exchange
TLS	Hybrid	Medium	Yes	Eavesdropping, tampering

Overall, the discourse surrounding enhancing IoT security through WSNs is vital for addressing the evolving challenges of a hyper-connected world, as stakeholders seek to protect critical infrastructure and user data from increasingly sophisticated cyber adversaries. By exploring innovative solutions and best practices, researchers and practitioners aim to create a more secure and resilient IoT environment that can withstand the test of time and technological advancements [19].

The Internet of Things (IoT) represents a transformative evolution in technology, connecting a multitude of devices to enhance automation and data exchange in various sectors, including healthcare, transportation, and smart homes. Despite its potential, the integration of IoT devices presents significant security challenges due to their inherent vulnerabilities across multiple layers, such as hardware, software, and network infrastructure.

As IoT devices proliferate, they often become targets for malicious attacks, including data theft, phishing, and Distributed Denial of Service (DDoS) attacks, leading to serious implications for both users and organizations. Wireless Sensor Networks (WSNs) play a crucial role in the functionality of IoT by enabling real-time monitoring and data collection through a distributed network of sensor nodes. These nodes are designed to observe and report on environmental conditions, thereby facilitating various applications, particularly in healthcare. However, the deployment of WSNs also introduces complexities in securing the devices and the data they handle.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

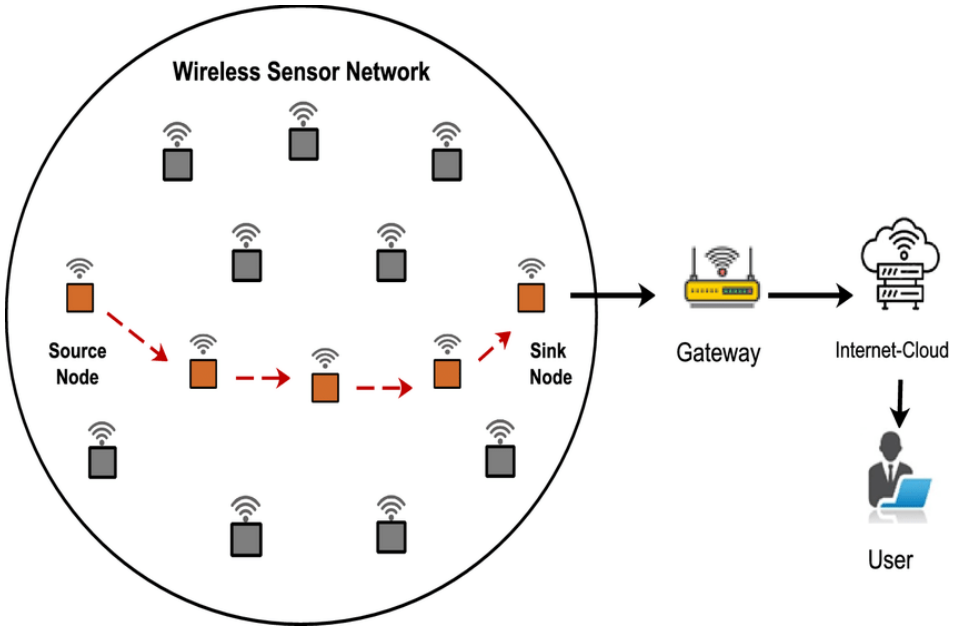

Figure 1: Secure IoT Network Architecture with WSNs [6]

Many IoT devices, particularly in medical settings, are found to have unpatched vulnerabilities, with studies indicating that 75% of infusion pumps and over 80% of imaging devices operate on outdated systems with known security flaws. The security landscape of IoT is further complicated by the necessity of balancing functionality with robust security measures. Implementing comprehensive security strategies, such as network segmentation and continuous monitoring, is essential for mitigating risks associated with device vulnerabilities. As connected devices become more integrated into everyday life, ensuring their security is critical not only for protecting sensitive data but also for safeguarding public health and safety.

The Internet of Things (IoT) introduces significant security challenges due to the interconnected nature of devices and the data they handle. These challenges arise from vulnerabilities that can be exploited by attackers, necessitating sophisticated security measures to protect both gateway and sensor nodes in the IoT network. One of the primary security risks in IoT is weak authentication. Many devices come with default or easily guessable passwords, which pose substantial security threats. If a password is not strong, it becomes a gateway for unauthorized access [9]. Moreover, a lack of robust authentication mechanisms can lead to devices being incorporated into botnets, where they can be used to execute distributed denial of service (DDoS) attacks, further exacerbating security concerns.

The nature of data transmission in IoT often involves public-access networks, making it vulnerable to interception. Attackers can eavesdrop on the communication channels, gaining access to sensitive information. To mitigate this, implementing encryption techniques like Transport Layer Security (TLS) and establishing secure Virtual Private Networks (VPNs) is essential for protecting data in transit.

Physical security of IoT devices is paramount, especially since many are deployed in remote or accessible locations. The risk of physical tampering or unauthorized access is significant, particularly for devices that store sensitive information, such as SIM cards. Utilizing resilient

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

components, like soldered eSIMs, can enhance the physical security of devices against such vulnerabilities.

Privacy remains a significant challenge, particularly with the potential for data leaks and tracking through IoT devices. As data is aggregated from various nodes, ensuring that sensitive information is not inadvertently exposed is critical. Privacy-preserving methods such as anonymization and pseudonymization can help protect users' identities and sensitive data from being traced back to their sources. The reliance on insecure communication protocols can expose IoT devices to various forms of attacks, such as denial of service, spoofing, and traffic analysis. Implementing secure data storage and transmission protocols is vital to counter these risks, ensuring that data remains confidential and protected against unauthorized access.

Literature Review:

The rapid advancement of the Internet of Things (IoT) has led to a proliferation of interconnected devices across critical sectors such as healthcare, smart cities, and industrial automation. This development, while enhancing efficiency and data exchange, has introduced significant security vulnerabilities. A substantial body of literature has emerged focusing on these security gaps, particularly in the context of Wireless Sensor Networks (WSNs), which form the backbone of many IoT implementations [20].

Numerous studies have identified that the majority of IoT devices [21] suffer from poor security configurations, including default passwords, outdated firmware, and weak authentication mechanisms. For instance, research in the healthcare sector has revealed that over 75% of infusion pumps and 80% of imaging devices are operating on outdated systems, leaving them susceptible to cyber threats such as unauthorized access, data breaches, and ransomware attacks [21].

Wireless Sensor Networks (WSNs), being integral to IoT environments, introduce specific vulnerabilities due to their decentralized nature, limited power resources, and physical deployment in exposed environments [22]. Prior works have emphasized the necessity of lightweight yet robust cryptographic protocols tailored for resource-constrained sensor nodes. Techniques such as Transport Layer Security (TLS), Virtual Private Networks (VPNs), and end-to-end encryption have been recommended to secure data transmission against eavesdropping and man-in-the-middle attacks [23].

The literature also addresses the importance of physical security in IoT deployments. Devices located in public or remote areas are at risk of tampering. Researchers have proposed hardware-based solutions such as soldered eSIMs to prevent unauthorized access to critical components [24]. Furthermore, privacy concerns have been highlighted with the aggregation of user data from multiple sources, necessitating anonymization and pseudonymization techniques to preserve user confidentiality [25].

Intrusion Detection Systems (IDS) have gained significant attention as a core defense mechanism for WSNs. Various IDS models have been proposed, ranging from rule-based to behavior-based systems. The use of Machine Learning (ML) and Artificial Intelligence (AI) in IDS has been particularly promising [26]. Studies incorporating Particle Swarm Optimization (PSO) in combination with classifiers such as Artificial Neural Networks (ANN) have achieved high detection accuracy and low false positive rates, surpassing traditional detection methods [27].

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

Emerging trends in the literature also point to the integration of blockchain technology as a decentralized solution for securing WSNs. Blockchain's immutability and transparency can enhance trust and prevent data tampering within distributed sensor environments [28]. The Zero Trust Architecture (ZTA) model, which enforces strict identity verification for every access request, is another contemporary framework gaining traction in the academic and professional discourse [29].

Despite these advances, challenges remain. Many researchers emphasize the difficulty of balancing performance with security in low-power, heterogeneous IoT systems. Additionally, the evolving nature of cyber threats demands continuous innovation in security frameworks, adaptive protocols, and user education.

The literature converges on the need for a multi-layered, adaptive, and intelligence-driven approach to securing IoT systems through WSNs. While technologies such as encryption, IDS, blockchain, and AI offer viable solutions, the dynamic and complex nature of IoT security continues to present a fertile ground for further research and development.

Methodology:

Proposed Framework for Enhancing IoT Security:

Enhancing Security through Wireless Sensor Networks

Wireless sensor networks (WSNs) play a pivotal role in enhancing security within the broader context of the Internet of Things (IoT). Given the increasing prevalence of IoT applications, the necessity for robust security measures to safeguard sensitive data has become paramount. This section explores the importance of intrusion detection systems (IDS) in securing WSNs and the associated challenges and best practices.

Importance of Intrusion Detection Systems

Intrusion detection systems are essential for protecting WSNs and IoT environments from various threats and vulnerabilities [30].In practical applications, intrusion detection is a common concern, as these networks often manage sensitive information. The constant evolution of threats necessitates sophisticated security architectures capable of defending both gateway and sensor nodes against attacks. As such, the integration of effective IDS can significantly mitigate the risks posed by internal and external attacks, enhancing the overall security posture of WSNs [31].

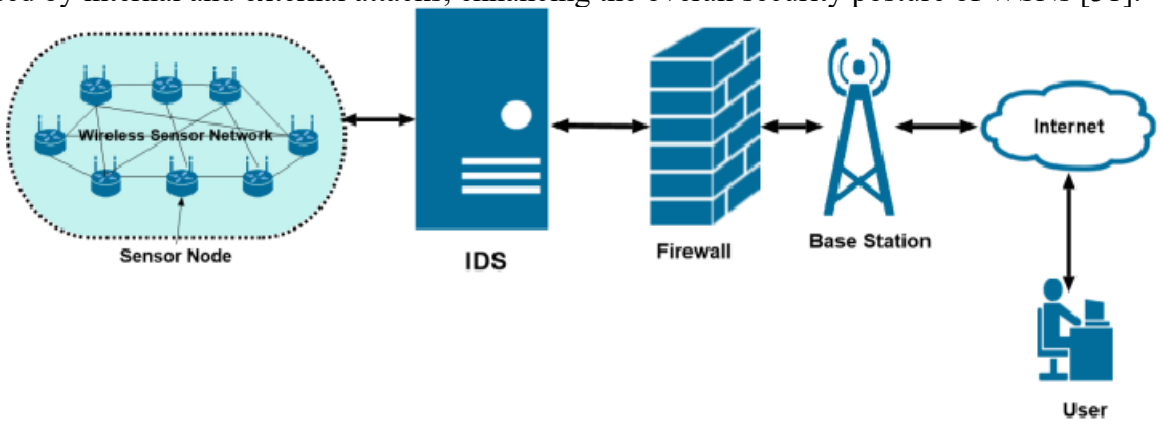

Figure 2: IDS Architecture for WSN [20]

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

Challenges in Securing Wireless Sensor Networks

Despite advancements in security measures, WSNs face numerous challenges in preserving data integrity and privacy. The dynamic nature of WSNs, characterized by frequently changing topologies due to node mobility or power constraints, complicates the implementation of consistent security protocols. Furthermore, the need for privacy-preserving data aggregation methods is critical; while aggregating data can reduce exposure to interception, ensuring that sensitive information remains confidential during this process poses significant challenges.

Privacy Risks and Vulnerabilities

Real-world incidents highlight the critical necessity for robust security in WSNs. For example, vulnerabilities in healthcare applications have exposed sensitive patient data, underscoring the urgent need for effective encryption and access control measures. The anonymity of data generated by sensor nodes is crucial for preventing attackers from tracing sensitive information back to its source. Techniques such as onion routing, where data is encrypted and relayed through multiple intermediary nodes, can help establish necessary anonymity within the network.

Best Practices for Securing WSNs

To address the myriad challenges faced by WSNs, several best practices have been proposed:
Layered Security Approach: Implementing security across multiple layers of the network physical, network, and application ensures a comprehensive defense against threats. Regular Key Management: Frequently updating cryptographic keys is essential to minimize the risk of key compromise, necessitating lightweight key management protocols tailored for WSNs. Continuous Monitoring and User Awareness: Establishing protocols for ongoing monitoring of network activity can help detect unusual behaviors indicative of privacy breaches. Additionally, educating users about potential threats is vital for maintaining a secure environment.

Results and Discussion:

Case Studies

Network Intrusion Detection Systems

In recent years, the importance of network intrusion detection systems (NIDS) has gained significant attention due to the increasing vulnerabilities of networks to various forms of attacks.

Table 2: ML-Based Intrusion Detection Performance

Model	Accuracy (%)	False Positive Rate (%)
PSO + ANN	99.78	0.003
PSO + KNN	97.45	0.071
PSO + Decision Trees	96.88	0.065

A study conducted using the Wireshark tool involved recording data packets during live communication within a simulation network created using Cisco Packet Tracer, alongside a real network configured with five node microcontroller units (MCUs), a laptop, and a mobile device. This setup allowed for the collection of datasets resulting from intentional intrusions. The datasets, which included standard datasets from sources such as UNSW, Kaggle, and GitHub, were subsequently used to train various machine learning (ML) models. An optimization technique known as Particle Swarm Optimization (PSO) was employed alongside ML classifiers, leading to notable results. Specifically, the combination of PSO with artificial neural networks (ANN)

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

achieved the highest accuracy of 99.78% and the lowest false positive rate (FPR) of 0.003%, outperforming other models like PSO+K-nearest neighbors (KNN) and PSO+decision trees (DT).

Intrusion Detection Categories

The landscape of intrusion detection systems can be categorized into three distinct types: hybrid IDS, exploitation identification, and anomaly detection. Hybrid IDS systems leverage both known and unknown attack detection mechanisms, while anomaly detection systems focus on identifying unidentified attacks by assessing the normal state of devices within the network. This distinction is crucial, as it influences the effectiveness and scope of threat detection capabilities within a network environment. Specifically, NIDS operates by analyzing traffic characteristics across the entire network to identify potential threats, providing a comprehensive overview of security risks without necessitating the use of all system capabilities for detection.

Evolving Security Challenges

The integration of IoT devices and wireless sensor networks (WSNs) in various applications has introduced new security challenges that necessitate advanced security architectures. Recent case studies have highlighted vulnerabilities in WSNs, such as matched protocol attacks, which exploit specific protocol structures to compromise network integrity. A proposed security framework aims to enhance performance through robust authentication methods and secure communication protocols, emphasizing the importance of implementing security measures throughout the design and operational phases of WSNs[33]. These studies underline the critical need for continuous adaptation and innovation in security practices to address the evolving threat landscape posed by IoT technologies and to ensure the resilience of network systems against potential breaches.

Future Trends

The future of security in IoT-based Wireless Sensor Networks (WSNs) is shaped by several emerging technologies and methodologies that aim to enhance resilience against cyber threats. As the integration of WSNs with advanced technologies such as artificial intelligence (AI), machine learning, and blockchain becomes more prevalent, their potential for improved security and efficiency grows substantially[34].

Advancements in Security Technologies

Artificial Intelligence and Machine Learning

AI and machine learning are set to revolutionize the security landscape of WSNs. These technologies can analyze vast amounts of data in real-time, identifying patterns and anomalies that may signify potential threats. The implementation of machine learning algorithms can lead to enhanced data aggregation and routing protocols, contributing to a more robust defense against cyber-attacks. Furthermore, AI-driven solutions can enable automated responses to detected breaches, significantly improving incident response times.

Blockchain Integration

Blockchain technology offers a decentralized framework that enhances WSN security by managing cryptographic keys and securing data transmissions. Its immutable nature helps create a tamper-resistant environment for handling sensitive information, thus boosting both privacy and security within WSNs. The capability of blockchain to provide an auditable trail of transactions enhances trust among network participants, addressing key vulnerabilities associated with traditional data management systems.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

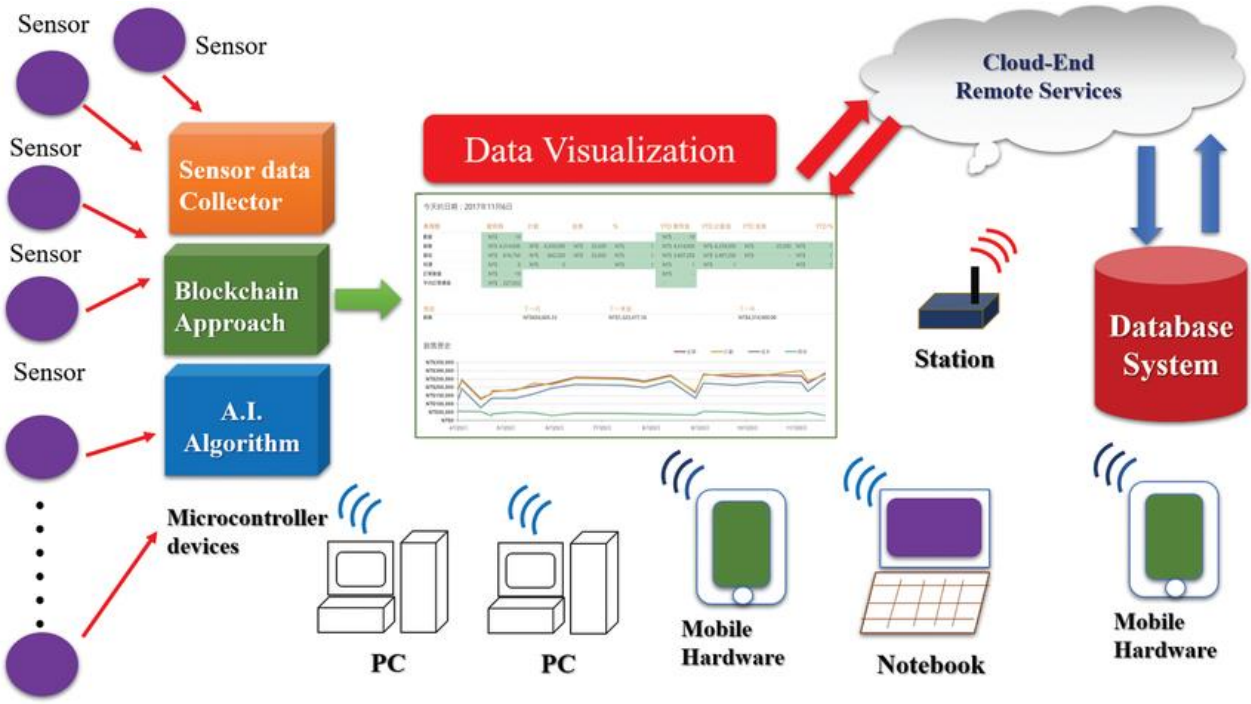

Figure 3: Blockchain-Integrated WSN Framework [35]

Enhancing Security Protocols

Cryptography and Encryption

The development of advanced cryptographic methods is crucial for securing WSNs. Techniques such as elliptic curve cryptography (ECC) and the Advanced Encryption Standard (AES) are gaining traction, especially for lightweight applications in the IoT domain. Moreover, hybrid encryption models and end-to-end protocols are essential for safeguarding communication between nodes and ensuring data integrity throughout the network [36].

Zero Trust Architecture

A Zero Trust security model is increasingly recognized as an effective approach for securing IoT devices and networks. This framework emphasizes the principle of "never trust, always verify," necessitating rigorous verification of all users and devices attempting to access the network, regardless of their location [37]. By adopting this model, organizations can mitigate risks associated with weak authentication and unauthorized access.

Challenges Ahead

Despite the advancements, challenges remain in the implementation of robust security measures for WSNs. The complexity of IoT environments, characterized by their vast scale and diversity of devices, poses significant hurdles in ensuring comprehensive security [38]. Moreover, the evolution of cyber threats requires continuous adaptation and enhancement of security protocols to prevent potential vulnerabilities from being exploited [39].

Conclusion:

Enhancing security in IoT through Wireless Sensor Networks (WSNs) remains a pressing need as the complexity and scale of connected devices expand across domains. This paper has highlighted the multifaceted nature of IoT vulnerabilities, ranging from weak authentication and outdated

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

systems to challenges in data privacy and intrusion detection. By implementing layered security architectures, deploying advanced encryption techniques, and integrating AI and blockchain, IoT systems can significantly strengthen their defenses. The experimental case studies reaffirm that combining machine learning models with optimization algorithms like PSO can yield highly accurate detection rates. However, future efforts must address evolving threats with adaptive frameworks, particularly those that accommodate heterogeneous devices and resource-constrained environments. Ultimately, the path forward requires a continuous commitment to innovation, collaboration, and best practices in cybersecurity to ensure a resilient and trustworthy IoT infrastructure.

References

[1] Zainab, Hira, Ali Raza A. Khan, Muhammad Ismaeel Khan, and Aftab Arif. "Ethical Considerations and Data Privacy Challenges in AI-Powered Healthcare Solutions for Cancer and Cardiovascular Diseases." Global Trends in Science and Technology 1, no. 1 (2025): 63-74.

[2] Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "The Most Recent Advances and Uses of AI in Cybersecurity." BULLET: Jurnal Multidisiplin Ilmu 3, no. 4 (2024): 566-578.

[3] "Cyber attack detection in IOT-WSN devices with threat intelligence using hidden and connected layer-based architectures | Journal of Cloud Computing | Full Text." Accessed: Aug. 02, 2025. [Online]. Available: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-024-00722-9

[4] Arif, Aftab, Muhammad Ismaeel Khan, and Ali Raza A. Khan. "An overview of cyber threats generated by AI." International Journal of Multidisciplinary Sciences and Arts 3, no. 4 (2024): 67-76.

[5] Arif, A., A. Khan, and M. I. Khan. "Role of AI in Predicting and Mitigating Threats: A Comprehensive Review." JURIHUM: Jurnal Inovasi dan Humaniora 2, no. 3 (2024): 297-311.

[6] "IoT Adoption in Healthcare Brings Security Opportunities - Perspectives." Accessed: Aug. 02, 2025. [Online]. Available: https://www.paloaltonetworks.com/perspectives/iot-adoption-in-healthcare/

[7] Tariq, Muhammad Arham, Muhammad Ismaeel Khan, Aftab Arif, Muhammad Aksam Iftikhar, and Ali Raza A. Khan. "Malware Images Visualization and Classification With Parameter Tunned Deep Learning Model." Metallurgical and Materials Engineering 31, no. 2 (2025): 68-73.https://doi.org/10.63278/1336.

[8] "IoT Vulnerabilities and Attacks: SILEX Malware Case Study." Accessed: Aug. 02, 2025. [Online]. Available: https://www.mdpi.com/2073-8994/15/11/1978

[9] Ahmad, Israr, Fawad Nasim, Muhammad Furqan Khawaja, Syed Asad Ali Naqvi, and Hamayun Khan. "Enhancing IoT security and services based on generative artificial intelligence techniques: a systematic analysis based on emerging threats, challenges and future directions." Spectrum of engineering sciences 3, no. 2 (2025): 1-25.

[10] Khan, M. I., A. Arif, and A. R. A. Khan. "AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity." BIN: Bulletin of Informatics 2, no. 2 (2024): 248-61.

[11] Imtiaz, Ahsan, Danish Shehzad, Fawad Nasim, Muhammad Afzaal, Muhammad Rehman, and Ali Imran. "Analysis of cybersecurity measures for detection, prevention, and misbehaviour of social systems." In 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), pp. 1-7. IEEE, 2023.

[12] Zainab, Hira, Muhammad Ismaeel Khan, Aftab Arif, and Ali Raza A. Khan. "Development of Hybrid AI Models for Real-Time Cancer Diagnostics Using Multi-Modality Imaging (CT, MRI, PET)." Global Journal of Machine Learning and Computing 1, no. 1 (2025): 66-75.

[13] Zainab, Hira, Muhammad Ismaeel Khan, Aftab Arif, and Ali Raza A. Khan. "Deep Learning in Precision Nutrition: Tailoring Diet Plans Based on Genetic and Microbiome Data." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 1 (2025): 31-42.
[14] Zainab, Hira, Ali Raza A. Khan, Muhammad Ismaeel Khan, and Aftab Arif. "Innovative AI Solutions for Mental Health: Bridging Detection and Therapy." Global Journal of Emerging AI and Computing 1, no. 1 (2025): 51-58.
[15] Imtiaz, Ahsan, Danish Shehzad, Hussain Akbar, Muhammad Afzaal, Muhammad Zubair, and Fawad Nasim. "Blockchain technology the future of cybersecurity." In 2023 24th International Arab Conference on Information Technology (ACIT), pp. 1-5. IEEE, 2023.
[16] Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "AI's Revolutionary Role in Cyber Defense and Social Engineering." International Journal of Multidisciplinary Sciences and Arts 3, no. 4 (2024): 57-66.
[17] Khan, Ali Raza A., Muhammad Ismaeel Khan, and Aftab Arif. "AI in Surgical Robotics: Advancing Precision and Minimizing Human Error." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 1 (2025): 17-30.
[18] Azam, Muhammad, Fawad Nasim, Jawad Ahmad, and Sohail Masood Bhatti. "A Security Framework for Data Migration over the Cloud." Journal of Computing & Biomedical Informatics 7, no. 02 (2024).
[19] "Understanding Privacy Issues in Wireless Sensor Networks." Accessed: Aug. 02, 2025. [Online]. Available: https://www.azosensors.com/article.aspx?ArticleID=3111
[20] B. Mopuru and Y. Pachipala, "Advancing IoT Security: Integrative Machine Learning Models for Enhanced Intrusion Detection in Wireless Sensor Networks," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 4, Art. no. 4, Aug. 2024, doi: 10.48084/etasr.7641.
[21] M. U. Mushtaq, P. D. J. Hong, M. Owais, and D. S. A. Danso, "Enhancing Security and Energy Efficiency in Wireless Sensor Network Routing with IOT Challenges: A Thorough Review," *LC Int. J. STEM ISSN 2708-7123*, vol. 4, no. 3, Art. no. 3, Oct. 2023, doi: 10.5281/zenodo.10184917.
[22] D. Saha *, "Improving IoT Security in Wireless Sensor Networks," *Smart Internet Things*, vol. 1, no. 4, Art. no. 4, Dec. 2024, doi: 10.22105/siot.v1i4.138.
[23] K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, "A review paper on wireless sensor network techniques in Internet of Things (IoT)," *Mater. Today Proc.*, vol. 51, pp. 161–165, Jan. 2022, doi: 10.1016/j.matpr.2021.05.067.
[24] "Deep Learning-Infused Hybrid Security Model for Energy Optimization and Enhanced Security in Wireless Sensor Networks | SN Computer Science." Accessed: Aug. 02, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s42979-024-03193-6
[25] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues," *Sensors*, vol. 22, no. 13, Art. no. 13, Jan. 2022, doi: 10.3390/s22134730.
[26] S. Sharma and V. K. Verma, "An Integrated Exploration on Internet of Things and Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 124, no. 3, pp. 2735–2770, Jun. 2022, doi: 10.1007/s11277-022-09487-3.
[27] S. Karthic and S. M. Kumar, "Hybrid Optimized Deep Neural Network with Enhanced Conditional Random Field Based Intrusion Detection on Wireless Sensor Network," *Neural Process. Lett.*, vol. 55, no. 1, pp. 459–479, Feb. 2023, doi: 10.1007/s11063-022-10892-9.
[28] A. Jabbari and J. B. Mohasefi, "Improvement of a User Authentication Scheme for Wireless Sensor Networks Based on Internet of Things Security," *Wirel. Pers. Commun.*, vol. 116, no. 3, pp. 2565–2591, Feb. 2021, doi: 10.1007/s11277-020-07811-3.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 02 (2025)

[29] M. Karthikeyan, D. Manimegalai, and K. RajaGopal, "Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection," *Sci. Rep.*, vol. 14, no. 1, p. 231, Jan. 2024, doi: 10.1038/s41598-023-50554-x.
[30] S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks," *Optik*, vol. 273, p. 170419, Feb. 2023, doi: 10.1016/j.ijleo.2022.170419.
[31] "A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction | Scientific Reports." Accessed: Aug. 02, 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-87028-1
[32] "Review on Security Issues and Applications of Trust Mechanism in Wireless Sensor Networks - Xia - 2022 - Computational Intelligence and Neuroscience - Wiley Online Library." Accessed: Aug. 02, 2025. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1155/2022/3449428
[33] "(PDF) A case study of Internet of Things based on wireless sensor networks and smartphone." Accessed: Aug. 02, 2025. [Online]. Available: https://www.researchgate.net/publication/257840438_A_case_study_of_Internet_of_Things_based_on_wireless_sensor_networks_and_smartphone
[34] "Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection | Scientific Reports." Accessed: Aug. 02, 2025. [Online]. Available: https://www.nature.com/articles/s41598-023-50554-x
[35] "The proposed WSN with blockchain technology," ResearchGate. Accessed: Aug. 02, 2025. [Online]. Available: https://www.researchgate.net/figure/The-proposed-WSN-with-blockchain-technology_fig1_351030970
[36] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," *Sensors*, vol. 18, no. 9, p. 2796, Aug. 2018, doi: 10.3390/s18092796.
[37] "Security for IoT Sensor Networks: Building Management Case Study | CSRC." Accessed: Aug. 02, 2025. [Online]. Available: https://csrc.nist.gov/pubs/pd/2019/02/01/security-for-iot-sensor-networks/ipd
[38] M. U. F. Qaisar, W. Yuan, P. Bellavista, and H. Tabassum, "IoT and Wireless Sensor Networks (WSNs)," in *Empowering IoT: Reliability, Network Management, Sensing, and Probabilistic Charging in Wireless Sensor Networks: A Comprehensive Guide to IoT-Based WSN Network Optimization*, M. U. F. Qaisar, W. Yuan, P. Bellavista, and H. Tabassum, Eds., Singapore: Springer Nature, 2025, pp. 35–56. doi: 10.1007/978-981-96-6079-7_2.
[39] A. Velliangiri, "Security Challenges and Solutions in IoT-Based Wireless Sensor Networks," *J. Wirel. Sens. Netw. IoT*, vol. 1, no. 1, Art. no. 1, Jul. 2024, doi: 10.31838/WSNIOT/01.01.02.