International Journal of Multidisciplinary Research and Growth Evaluation.

AI-driven intrusion detection and threat modeling to prevent unauthorized access in smart manufacturing networks

Yewande Goodness Hassan [1*], Anuoluwapo Collins [2], Gideon Opeyemi Babatunde [3], Abidemi Adeleye Alabi [4], Sikirat Damilola Mustapha [4]

[1] Montclair State University, NJ, USA
[2] Cognizant Technology Solutions, Canada
[3] Cadillac Fairview, Ontario, Canada
[4] Independent Researcher, Texas, USA
[5] Montclair State University, Montclair, New Jersey, USA

* Corresponding Author: **Yewande Goodness Hassan**

Article Info

ISSN (online): 2582-7138
Volume: 05
Issue: 01
January-February 2024
Received: 19-12-2023
Accepted: 23-01-2024
Page No: 1197-1202

Abstract
The rapid adoption of Internet of Things (IoT) technologies in smart manufacturing has revolutionized production processes but has also introduced significant cybersecurity challenges. Cyber-physical systems, integral to modern manufacturing, are increasingly vulnerable to unauthorized access, data breaches, and operational disruptions. This paper explores the role of artificial intelligence (AI) in enhancing intrusion detection and threat modeling to secure these networks. By leveraging machine learning, deep learning, and predictive analytics, AI-driven solutions offer adaptive and real-time responses to evolving threats. The study highlights cybersecurity challenges, reviews state-of-the-art AI methodologies, and examines real-world implementations in diverse manufacturing environments. It also identifies key insights from successful deployments and discusses the potential for future advancements in scalability, real-time responsiveness, and resilience. This paper concludes by emphasizing the transformative potential of AI in building robust, secure, and efficient smart manufacturing systems while addressing the critical need for ongoing research and collaboration.

DOI: https://doi.org/10.54660/.IJMRGE.2024.5.1.1197-1202

Keywords: Artificial intelligence, intrusion detection systems, threat modeling, smart manufacturing, cybersecurity, internet of things

Introduction

Smart manufacturing represents the convergence of advanced manufacturing techniques and cutting-edge digital technologies (Solanki, 2023) [45]. With the advent of the Internet of Things (IoT), manufacturers can now achieve unprecedented levels of efficiency, automation, and precision. IoT facilitates interconnected devices, sensors, and systems that communicate and collaborate in real time, enabling predictive maintenance, production optimization, and resource management. This rapid adoption of IoT has become a hallmark of Industry 4.0, revolutionizing traditional manufacturing practices (Nain, Pattanaik, & Sharma, 2022) [25].

However, the increased reliance on interconnected networks also introduces significant vulnerabilities. Cyber-physical systems (CPS), which merge physical processes with computational controls, are particularly susceptible to unauthorized access (Humayed, Lin, Li, & Luo, 2017) [17]. Such vulnerabilities stem from IoT devices' open nature, extensive interconnectivity, and limited built-in security features. Addressing these security challenges is vital for ensuring manufacturing networks' integrity, availability, and confidentiality (Yaacoub *et al*., 2020) [47].

As the industrial sector integrates IoT on a larger scale, the risk of cyberattacks has risen exponentially. Unauthorized access to

manufacturing networks can result in data theft, operational disruptions, or even sabotage of physical processes (Stellios, Kotzanikolaou, Psarakis, Alcaraz, & Lopez, 2018) [46].

The highly dynamic nature of manufacturing environments, with their heterogeneous devices and real-time communication requirements, exacerbates the difficulty of detecting and mitigating threats. Traditional security mechanisms designed for static IT infrastructures often fail to address these evolving challenges, exposing smart factories to sophisticated cyber threats (Djenna, Harous, & Saidouni, 2021) [16].

Artificial intelligence (AI) offers transformative potential in enhancing cybersecurity for smart manufacturing networks. By leveraging machine learning (ML), deep learning, and other AI-based techniques, intrusion detection systems (IDS) can identify and respond to threats with greater accuracy and adaptability (Manoharan & Sarker, 2023) [24]. Additionally, AI-driven threat modeling enables manufacturers to proactively anticipate potential attack vectors and reinforce vulnerable points in their networks. This paper explores how these technologies can be harnessed to secure IoT-enabled manufacturing environments (De Azambuja *et al*., 2023) [15].

This review focuses on key intrusion detection and threat modeling aspects within smart manufacturing networks. It examines the role of AI techniques in identifying unauthorized access, discusses contemporary approaches to threat modeling, and highlights the challenges and opportunities presented by integrating AI into manufacturing cybersecurity frameworks. Through this exploration, the paper aims to comprehensively understand how AI-driven methods can address the pressing need for robust and adaptive security solutions.

2. State of the Art in Smart Manufacturing Cybersecurity

2.1 Cybersecurity Challenges in Smart Manufacturing and Existing Solutions

The integration of IoT and cyber-physical systems (CPS) in smart manufacturing has introduced unique cybersecurity challenges. Unlike traditional IT systems, these environments operate at the intersection of physical and digital domains, where security breaches can have both digital and physical consequences (Kayan, Nunes, Rana, Burnap, & Perera, 2022) [23]. The diversity and scale of connected devices in manufacturing networks create numerous entry points for attackers. Many of these devices, designed for efficiency and functionality, often lack robust security protocols, making them prime targets for exploitation (Chukwurah, Ige, Idemudia, & Adebayo, 2024) [14].

One critical vulnerability is the heterogeneity of devices, which often originate from multiple vendors with varying security standards. This lack of standardization complicates the implementation of unified security measures. Additionally, real-time data transmission between devices and systems is essential for manufacturing operations but opens pathways for attacks such as data interception, spoofing, and denial-of-service. The dynamic nature of manufacturing processes, which frequently involve changes in production lines and the addition of new devices, further amplifies these risks (Onoja & Ajala, 2024) [37].

Another key challenge lies in the convergence of IT and operational technology (OT). While IT systems traditionally focus on data confidentiality and integrity, OT systems prioritize availability and uptime. This fundamental difference in priorities creates security gaps that cybercriminals can exploit. Furthermore, the consequences of a successful attack in smart manufacturing extend beyond financial loss, including production downtime, compromised product quality, and risks to personnel safety (Afolabi, Ige, Akinade, & Adepoju, 2023; Alonge, Dudu, & Alao, 2024b) [11, 25].

Traditional intrusion detection systems (IDS) have been deployed in manufacturing networks to address these challenges. These systems aim to monitor network activity, detect anomalies, and flag potential threats. IDS operate using either signature-based detection, which relies on known patterns of malicious behavior, or anomaly-based detection, which identifies deviations from established baselines (Osundare, Ike, Fakeyede, & Ige, 2024e) [48].

While effective in conventional IT environments, traditional IDS face significant limitations in the dynamic and heterogeneous context of smart manufacturing. Signature-based detection systems struggle to keep up with the rapid evolution of attack techniques, often missing new or unknown threats. Anomaly-based systems, while more adaptable, can generate high rates of false positives, leading to alert fatigue and reduced efficiency. Moreover, traditional IDS are not well-equipped to handle the volume and velocity of data generated in manufacturing environments. Real-time monitoring and analysis of such vast datasets require computational capabilities beyond what conventional methods can provide. These limitations highlight the need for more adaptive and intelligent solutions tailored to the specific demands of smart manufacturing cybersecurity (Ishola, Odunaiya, & Soyombo, 2024; Onoja & Ajala, 2023b) [22, 36].

2.2 Emerging Trends

To overcome the shortcomings of traditional approaches, the adoption of artificial intelligence (AI) and machine learning (ML) has emerged as a promising trend in smart manufacturing cybersecurity. AI-driven systems bring a level of adaptability and intelligence essential for managing modern manufacturing networks' complexities (Bécue, Praça, & Gama, 2021) [13]. One key advantage of AI is its ability to process and analyze large volumes of data in real time, identifying patterns and anomalies that might indicate a potential threat. Unlike traditional methods, AI can learn from data over time, improving its accuracy and reducing false positives. For example, ML algorithms can be trained on historical data to recognize normal operational behavior and flag deviations that may signify unauthorized access or malicious activity (Ike *et al*., 2021; Oladosu *et al*., 2022c) [24].

Deep learning, a subset of AI, offers even greater potential for enhancing intrusion detection. By leveraging neural networks, deep learning models can identify subtle and complex patterns in data that traditional systems might overlook. These models can adapt to evolving threats, making them particularly effective in dynamic manufacturing environments.

In addition to intrusion detection, AI is being integrated into threat modeling to anticipate and mitigate potential vulnerabilities. Predictive analytics powered by AI allows manufacturers to simulate attack scenarios, identify weak points in their systems, and implement proactive security measures. This forward-looking approach enhances the resilience of manufacturing networks and reduces the risk of costly and disruptive attacks (Manoharan & Sarker, 2023) [24].

Another notable trend is the incorporation of AI with edge

computing. In manufacturing environments, where latency and real-time responsiveness are critical, processing data locally at the network's edge enables faster detection and response to threats. This approach minimizes the reliance on centralized systems, which can become bottlenecks or single points of failure (George, Idemudia, & Ige, 2024b; Oladosu *et al*., 2022b) [33, 48].

Despite its promise, integrating AI in cybersecurity is not without challenges. The development and deployment of AI-driven systems require significant expertise and resources. Additionally, these systems are not immune to adversarial attacks, where attackers manipulate input data to deceive the AI models. Addressing these challenges is essential for realizing the full potential of AI in securing smart manufacturing networks. In summary, while smart manufacturing faces significant cybersecurity challenges, the evolution from traditional methods to AI-driven solutions marks a transformative shift. These emerging technologies address existing systems' limitations and pave the way for more robust and adaptive security frameworks, ensuring the resilience of manufacturing operations in an increasingly connected world (Oladosu *et al*., 2022a; Osundare & Ige, 2024b) [32, 48].

3. AI-Driven Intrusion Detection and Threat Modeling

3.1 AI Techniques for Intrusion Detection

Artificial intelligence has revolutionized how intrusion detection systems (IDS) function by enhancing their ability to detect, analyze, and respond to cyber threats. Among the core techniques used in AI-driven intrusion detection are supervised, unsupervised, and reinforcement learning approaches, each contributing uniquely to improving system performance (Aminu, Akinsanya, Dako, & Oyedokun, 2024). Supervised learning relies on labeled datasets to train models that can classify network activities as benign or malicious. This method identifies known attack patterns, making it highly effective in environments with well-documented threats. However, its dependency on labeled data limits its ability to detect novel threats. In contrast, unsupervised learning does not require labeled data and instead focuses on identifying anomalies within network activity (Afolabi, Hussain, Austin-Gabriel, Adepoju, & Ige, 2023) [11]. By clustering similar patterns and flagging deviations, unsupervised methods can detect previously unknown threats, though they may produce false positives. Reinforcement learning, which involves training an agent to make decisions by rewarding desirable outcomes, offers a dynamic approach to intrusion detection. It can adapt to changes in network behavior and optimize its responses over time, making it suitable for highly dynamic environments (Alonge, Dudu, & Alao, 2024a; Onoja & Ajala, 2022) [33, 8].

Deep learning, a subset of AI, has emerged as a powerful tool in intrusion detection. Neural networks used in deep learning models can process vast amounts of data to identify complex patterns and correlations that traditional methods might overlook. These models are particularly effective in anomaly detection, where they analyze network activity to establish baselines of normal behavior and flag deviations. By leveraging techniques such as autoencoders and convolutional neural networks, deep learning can enhance the accuracy and efficiency of IDS, reducing false positives and improving threat detection capabilities (Adepoju *et al*., 2022; Osundare, Ike, Fakeyede, & Ige, 2024d) [50].

3.2 Threat Modeling in Smart Manufacturing

Threat modeling is crucial in identifying, assessing, and mitigating potential vulnerabilities in smart manufacturing networks. It provides a systematic approach to understanding how adversaries might exploit weaknesses in a system and enables the development of proactive security measures. Several established frameworks and methodologies, such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) and ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), are widely used in this context (Ofoegbu, Osundare, Ike, Fakeyede, & Ige, 2024) [47].

STRIDE offers a structured way to identify potential threats by categorizing them into specific types, each associated with a set of mitigation strategies. For example, it highlights risks such as data tampering and unauthorized access, which are particularly relevant to IoT-enabled manufacturing environments. ATT&CK, on the other hand, provides a comprehensive knowledge base of adversarial tactics and techniques. By mapping observed attack patterns to the framework, manufacturers can gain valuable insights into attackers' behavior and strengthen their defenses accordingly (Oladosu *et al*., 2024; Osundare, Ike, Fakeyede, & Ige, 2024c) [49, 35].

AI enhances threat modeling by enabling predictive analytics and automating the identification of vulnerabilities. Predictive models powered by machine learning can simulate potential attack scenarios and provide actionable insights into areas requiring immediate attention. This capability allows manufacturers to proactively address vulnerabilities before they can be exploited, reducing the risk of breaches. Additionally, AI algorithms can continuously analyze threat intelligence data from multiple sources, ensuring that the threat model remains up-to-date with emerging risks (Osundare & Ige, 2024a) [47].

3.3 Integration of AI and IoT in Smart Manufacturing

The integration of AI with IoT has brought significant advancements in real-time security mechanisms for smart manufacturing networks. AI-driven systems excel at processing and analyzing the large volumes of data generated by IoT devices, enabling timely detection and response to security incidents. This capability is critical in manufacturing environments where a brief disruption can result in substantial financial losses or safety hazards (Sharma, Sharma, & Grover, 2024) [44].

One key advantage of AI-driven security mechanisms is their ability to adapt to the dynamic nature of IoT-enabled manufacturing networks. Unlike traditional systems requiring manual updates to address new threats, AI systems can learn and evolve autonomously. For instance, anomaly detection models can adjust to changes in network behavior caused by the addition of new devices or shifts in production processes. This adaptability ensures that the security framework remains effective in the face of constant changes (Alao, Dudu, Alonge, & Eze, 2024; George, Idemudia, & Ige, 2024a) [8, 48].

However, the integration of AI and IoT also presents challenges. The resource-intensive nature of AI algorithms, particularly those used in deep learning, demands significant computational power. Implementing such systems in resource-constrained environments may require the adoption of edge computing, where data processing occurs locally rather than in centralized servers. While edge computing

reduces latency and enhances real-time responsiveness, it also introduces new security considerations, such as ensuring the integrity of data processed at the edge (Onoja & Ajala, 2023a) [34].

Additionally, the effectiveness of AI-driven systems depends on the quality and diversity of the data used for training. Manufacturing networks often involve proprietary processes and unique configurations, making developing customized models tailored to specific environments essential. Addressing these challenges requires collaboration between manufacturers, cybersecurity experts, and AI researchers to design solutions that balance security, efficiency, and scalability (Adebayo, Ige, Idemudia, & Eyieyien, 2024) [1].

4. Real-world Applications

4.1 Practical Implementations

The application of artificial intelligence (AI) in intrusion detection systems (IDS) and threat modeling has seen growing adoption in smart manufacturing, with several notable real-world implementations demonstrating its effectiveness. These case studies illustrate how AI-driven security solutions address the unique challenges of modern manufacturing networks (Alohali *et al*., 2022).

One such example is deploying AI-powered security systems in automotive manufacturing facilities, where interconnected robots and sensors are integral to production processes. In these environments, machine learning (ML) algorithms monitor network traffic, identify anomalies, and prevent potential breaches. By leveraging historical data, these systems detect deviations from normal communication patterns between devices, allowing operators to respond to threats before they escalate. This proactive approach has significantly reduced downtime caused by cyberattacks, ensuring uninterrupted production workflows (Osundare, Ike, Fakeyede, & Ige, 2024a) [48].

Similarly, deep learning-based IDS have been implemented in the electronics manufacturing industry to safeguard sensitive intellectual property. With manufacturing networks often targeted by attackers seeking to steal proprietary designs, companies have employed AI models capable of identifying subtle patterns indicative of advanced persistent threats. These systems continuously analyze vast data streams, including encrypted communications, to detect suspicious activities that traditional methods might overlook. This has enhanced the protection of intellectual property while maintaining the efficiency of production processes (Adepoju *et al*., 2022; Austin-Gabriel, Hussain, Ige, Adepoju, & Afolabi, 2023) [11].

Another noteworthy implementation is the use of AI in pharmaceutical manufacturing, where regulatory compliance and product integrity are critical. Threat modeling frameworks, augmented by AI, are applied to simulate potential attack scenarios and prioritize vulnerabilities based on their likelihood and impact. For example, predictive analytics tools can identify risks associated with unauthorized access to process control systems, enabling manufacturers to implement targeted security measures. The integration of these tools has improved cybersecurity and demonstrated compliance with stringent regulatory standards, bolstering the industry's resilience against cyber threats (Ige, Chukwurah, Idemudia, & Adebayo, 2024) [14].

4.2 Key Insights

The success of these implementations provides valuable lessons and insights into deploying AI-based IDS and threat modeling in smart manufacturing. One key takeaway is the importance of customization. Manufacturing networks are highly diverse, with each facility possessing unique configurations, device ecosystems, and operational workflows. As a result, off-the-shelf AI solutions often fail to address specific security needs. Successful deployments have involved tailoring AI models to the nuances of the target environment, including training algorithms on facility-specific data and integrating them with existing security protocols.

Another critical insight is the necessity of balancing automation with human oversight. While AI systems excel at identifying patterns and anomalies, they are not infallible. Though reduced compared to traditional methods, false positives remain a challenge, particularly in environments with highly dynamic network behaviors. To address this, many manufacturers have adopted a hybrid approach, where AI systems handle initial threat detection, and human analysts review flagged incidents for accuracy. This collaboration enhances the overall reliability of the security framework and builds trust in AI-driven solutions (Ojukwu *et al*., 2024; Oladosu *et al*., 2021) [32, 37].

The role of data quality cannot be overstated. Effective AI systems depend on diverse and high-quality datasets for training and validation. In several case studies, manufacturers highlighted the challenges of acquiring comprehensive datasets that accurately represent the complexity of their networks. Addressing this issue requires investing in robust data collection and preprocessing mechanisms to ensure that AI models perform optimally. Additionally, ongoing updates to datasets are essential for maintaining the relevance and accuracy of AI systems in evolving threat landscapes.

Despite the successes, several challenges remain. One notable issue is the scalability of AI-based solutions in large manufacturing environments. Processing the vast amounts of data generated by IoT devices and control systems demands significant computational resources. Many organizations have addressed this by adopting distributed computing architectures, such as edge computing, to process data locally and reduce latency (Osundare, Ike, Fakeyede, & Ige, 2024b) [48]. However, implementing such architectures introduces new technical and security challenges that must be carefully managed. Furthermore, adversarial attacks on AI systems themselves pose a growing concern. Sophisticated attackers may exploit vulnerabilities in machine learning algorithms to manipulate their outputs or evade detection altogether. This has prompted the need for research into adversarial resilience, ensuring that AI systems remain robust against such tactics. Manufacturers must incorporate these considerations into their long-term cybersecurity strategies to maintain the effectiveness of their defenses (Akinade, Adepoju, Ige, Afolabi, & Amoo, 2022; Austin-Gabriel *et al*., 2021) [15].

5. Conclusion and Recommendations

The adoption of artificial intelligence (AI) in intrusion detection and threat modeling represents a significant advancement in securing smart manufacturing networks. This paper has explored how AI-driven solutions address the unique cybersecurity challenges of integrating interconnected devices and systems in modern manufacturing. AI techniques, such as supervised, unsupervised, and reinforcement learning, enhance the detection of known and emerging threats, while deep learning

models provide sophisticated anomaly detection capabilities. Moreover, AI in threat modeling enables manufacturers to predict vulnerabilities and implement proactive security measures, improving overall network resilience. Real-world applications of these technologies have demonstrated their effectiveness in safeguarding manufacturing processes, intellectual property, and regulatory compliance despite the complexities of dynamic and heterogeneous environments.

While the benefits of AI-driven solutions are undeniable, there are several areas for improvement to ensure their long-term success and adoption. One key area is the refinement of AI methodologies to enhance their accuracy and reduce false positives. Developing advanced algorithms that distinguish between benign and malicious anomalies more effectively will minimize alert fatigue and improve operational efficiency.

Another priority is scalability. As manufacturing networks grow in size and complexity, AI systems must be capable of processing and analyzing vast amounts of data in real time. This requires more efficient algorithms and innovative architectures, such as distributed or edge computing, to handle the computational demands. Ensuring seamless integration of AI systems with existing network infrastructures will also be essential for widespread adoption.

Real-time responsiveness is another critical aspect that demands attention. Manufacturing environments operate on tight schedules, where even minor delays can lead to significant disruptions. AI systems must be optimized for timely threat detection and response without compromising performance. Additionally, enhancing the resilience of AI-driven systems against adversarial attacks will be crucial to maintaining their effectiveness in the face of increasingly sophisticated cyber threats.

To address these challenges, collaboration between academia, industry, and government agencies is necessary. Research initiatives should focus on developing standardized frameworks for AI implementation in manufacturing cybersecurity, ensuring interoperability and consistency across different systems. Training programs and knowledge-sharing platforms can also help bridge the skills gap, enabling manufacturers to effectively deploy and manage AI-based security solutions.

6. References

1. Adebayo VI, Ige AB, Idemudia C, Eyieyien OG. Ensuring compliance with regulatory and legal requirements through robust data governance structures. Open Access Res J Multidiscip Stud. 2024;8(1):036–44. DOI:10.53022/oarjms.2024.8.1.0043.
2. Adepoju PA, Austin-Gabriel B, Ige AB, Hussain NY, Amoo OO, Afolabi AI. Machine learning innovations for enhancing quantum-resistant cryptographic protocols in secure communication. Open Access Res J Multidiscip Stud. 2022. DOI:10.53022/oarjms.2022.4.1.0075.
3. Afolabi AI, Hussain NY, Austin-Gabriel B, Adepoju PA, Ige AB. Geospatial AI and data analytics for satellite-based disaster prediction and risk assessment. Open Access Res J Eng Technol. 2023. DOI:10.53022/oarjet.2023.4.2.0058.
4. Afolabi AI, Ige AB, Akinade AO, Adepoju PA. Virtual reality and augmented reality: A comprehensive review of transformative potential in various sectors. Magna Scientia Adv Res Rev. 2023. DOI:10.30574/msarr.2023.7.2.0039.
5. Akinade AO, Adepoju PA, Ige AB, Afolabi AI, Amoo OO. Advancing segment routing technology: A new model for scalable and low-latency IP/MPLS backbone optimization.
6. Alao OB, Dudu OF, Alonge EO, Eze CE. Automation in financial reporting: A conceptual framework for efficiency and accuracy in US corporations. Glob J Adv Res Rev. 2024;2(2):040–50.
7. Alohali MA, Al-Wesabi FN, Hilal AM, Goel S, Gupta D, Khanna A. Artificial intelligence-enabled intrusion detection systems for cognitive cyber-physical systems in Industry 4.0 environment. Cogn Neurodynamics. 2022;16(5):1045–57.
8. Alonge EO, Dudu OF, Alao OB. The impact of digital transformation on financial reporting and accountability in emerging markets. Int J Sci Technol Res Arch. 2024;7(2):025–49.
9. Alonge EO, Dudu OF, Alao OB. Utilizing advanced data analytics to boost revenue growth and operational efficiency in technology firms.
10. Aminu M, Akinsanya A, Dako DA, Oyedokun O. Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. Int J Comput Appl Technol Res. 2024;13(8):11–27.
11. Austin-Gabriel B, Hussain NY, Ige AB, Adepoju PA, Afolabi AI. Natural language processing frameworks for real-time decision-making in cybersecurity and business analytics. Int J Sci Technol Res Arch. 2023. DOI:10.53771/ijstra.2023.4.2.0018.
12. Austin-Gabriel B, Hussain NY, Ige AB, Adepoju PA, Amoo OO, Afolabi AI. Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. Open Access Res J Eng Technol. 2021. DOI:10.53022/oarjet.2021.1.1.0107.
13. Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artif Intell Rev. 2021;54(5):3849–86.
14. Chukwurah N, Ige AB, Idemudia C, Adebayo VI. Strategies for engaging stakeholders in data governance: Building effective communication and collaboration. Open Access Res J Multidiscip Stud. 2024;8(1):057–67. DOI:10.53022/oarjms.2024.8.1.0045.
15. De Azambuja AJG, Plesker C, Schützer K, Anderl R, Schleich B, Almeida VR. Artificial intelligence-based cybersecurity in the context of industry 4.0—a survey. Electronics. 2023;12(8):1920.
16. Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Appl Sci. 2021;11(10):4580.
17. George EP-E, Idemudia C, Ige AB. Blockchain technology in financial services: Enhancing security, transparency, and efficiency in transactions and services. Open Access Res J Multidiscip Stud. 2024;8(1):026–35. DOI:10.53022/oarjms.2024.8.1.0042.
18. George EP-E, Idemudia C, Ige AB. Recent advances in implementing machine learning algorithms to detect and prevent financial fraud in real-time. Int J Eng Res Dev. 2024;20(7).
19. Humayed A, Lin J, Li F, Luo B. Cyber-physical systems security—A survey. IEEE Internet Things J. 2017;4(6):1802–31.
20. Ige AB, Chukwurah N, Idemudia C, Adebayo VI. Managing data lifecycle effectively: Best practices for

data retention and archival processes. Int J Eng Res Dev. 2024;20(8):199–207.
21. Ike CC, Ige AB, Oladosu SA, Adepoju PA, Amoo OO, Afolabi AI. Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement.
22. Ishola AO, Odunaiya OG, Soyombo OT. Stakeholder communication framework for successful implementation of community-based renewable energy projects.
23. Kayan H, Nunes M, Rana O, Burnap P, Perera C. Cybersecurity of industrial cyber-physical systems: A review. ACM Comput Surv. 2022;54(11s):1–35.
24. Manoharan A, Sarker M. Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. IRJMETS. 2023;1:10.56726/IRJMETS32644.
25. Nain G, Pattanaik K, Sharma G. Towards edge computing in intelligent manufacturing: Past, present and future. J Manuf Syst. 2022;62:588–611.
26. Ofoegbu KDO, Osundare OS, Ike CS, Fakeyede OG, Ige AB. Empowering users through AI-driven cybersecurity solutions: Enhancing awareness and response capabilities. Open Access Eng Sci Technol J. 2024;4(6):707–27. DOI:10.51594/estj.v4i6.1528.
27. Ojukwu PU, Cadet E, Osundare OS, Fakeyede OG, Ige AB, Uzoka A. Advancing green bonds through FinTech innovations: A conceptual insight into opportunities and challenges. Int J Eng Res Dev. 2024;20:565–76.
28. Oladosu SA, Ige AB, Ike CC, Adepoju PA, Amoo OO, Afolabi AI. Next-generation network security: Conceptualizing a unified, AI-powered security architecture for cloud-native and on-premise environments. Int J Sci Technol Res Arch. 2022;3(2):270–80. DOI:10.53771/ijstra.2022.3.2.0143.
29. Oladosu SA, Ige AB, Ike CC, Adepoju PA, Amoo OO, Afolabi AI. Reimagining multi-cloud interoperability: A conceptual framework for seamless integration and security across cloud platforms. Open Access Res J Sci Technol. 2022. DOI:10.53022/oarjst.2022.4.1.0026.
30. Oladosu SA, Ige AB, Ike CC, Adepoju PA, Amoo OO, Afolabi AI. Revolutionizing data center security: Conceptualizing a unified security framework for hybrid and multi-cloud data centers. Open Access Res J Sci Technol. 2022. DOI:10.53022/oarjst.2022.5.2.0065.
31. Oladosu SA, Ike CC, Adepoju PA, Afolabi AI, Ige AB, Amoo OO. Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premise integrations.
32. Oladosu SA, Ike CC, Adepoju PA, Afolabi AI, Ige AB, Amoo OO. Frameworks for ethical data governance in machine learning: Privacy, fairness, and business optimization.
33. Onoja JP, Ajala OA. Innovative telecommunications strategies for bridging digital inequities: A framework for empowering underserved communities. GSC Adv Res Rev. 2022;13(1):210–7. DOI:10.30574/gscarr.2022.13.1.0286.
34. Onoja JP, Ajala OA. AI-driven project optimization: A strategic framework for accelerating sustainable development outcomes. GSC Adv Res Rev. 2023;15(1):158–65. DOI:10.30574/gscarr.2023.15.1.0118.
35. Onoja JP, Ajala OA. Smart city governance and digital platforms: A framework for inclusive community engagement and real-time decision-making. GSC Adv Res Rev. 2023;15(3):310–7. DOI:10.30574/gscarr.2023.15.3.0225.
36. Onoja JP, Ajala OA. Synergizing AI and telecommunications for global development: A framework for achieving scalable and sustainable development. Comput Sci IT Res J. 2024;5(12):2703–14. DOI:10.51594/csitrj.v5i12.1776.
37. Osundare OS, Ige AB. Developing a robust security framework for inter-bank data transfer systems in the financial service sector. Int J Scholarly Res Sci Technol. 2024;5(1).
38. Osundare OS, Ige AB. Optimizing network performance in large financial enterprises using BGP and VRF-lite. Int J Scholarly Res Sci Technol. 2024;5(1).
39. Osundare OS, Ike CS, Fakeyede OG, Ige AB. Active/Active data center strategies for financial services: Balancing high availability with security. Open Access Comput Sci IT Res J. 2024;3(2):92–114. DOI:10.51594/csitrj.v3i3.1494.
40. Osundare OS, Ike CS, Fakeyede OG, Ige AB. Application of machine learning in detecting fraud in telecommunication-based financial transactions. Open Access Comput Sci IT Res J. 2024;4(3):458–77. DOI:10.51594/csitrj.v4i3.1499.
41. Osundare OS, Ike CS, Fakeyede OG, Ige AB. Evaluating core router technology upgrades: Case studies from telecommunications and finance. Open Access Comput Sci IT Res J. 2024;4(3):416–35. DOI:10.51594/csitrj.v4i3.1497.
42. Osundare OS, Ike CS, Fakeyede OG, Ige AB. IPv6 implementation strategies: Insights from the telecommunication and finance sectors. Open Access Eng Sci Technol J. 2024;4(6):672–88. DOI:10.51594/estj.v4i6.1526.
43. Osundare OS, Ike CS, Fakeyede OG, Ige AB. Secure communication protocols for real-time interbank settlements. Open Access Comput Sci IT Res J. 2024;4(3):436–57. DOI:10.51594/csitrj.v4i3.1498.
44. Sharma S, Sharma K, Grover S. Real-time data analysis with smart sensors. In: Application of Artificial Intelligence in Wastewater Treatment. Springer; 2024. p. 127–53.
45. Solanki SM. Industry 4.0 and smart manufacturing: Exploring the integration of advanced technologies in manufacturing. Rev Index J Multidiscip. 2023;3(2):36–46.
46. Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J. A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Commun Surv Tutorials. 2018;20(4):3453–95.
47. Yaacoub J-PA, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors Microsyst. 2020;77:103201