International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 13, Issue 12 [December. 2024] PP: 01-06

Enhancing Smart Manufacturing Supply Chains Through Cybersecurity Measures

Nwankwo Constance Obiuto[1], Okpala Charles Chikwendu[2], Igbokwe Nkemakonam Chidiebube[3]
[1,2,3]Faculty of Engineering, Industrial/Production Engineering Department
Nnamdi Azikiwe University, Awka, Nigeria.

Abstract
This review paper examines the critical intersection of cybersecurity and smart manufacturing supply chains, underscoring the paramount importance of cybersecurity measures in the era of digital manufacturing. As smart manufacturing integrates advanced digital technologies such as IoT, AI, and blockchain, it faces increased cybersecurity risks, including data breaches and unauthorized access, which can significantly disrupt operations. The paper outlines best practices, advanced technological solutions, and a comprehensive framework for enhancing cybersecurity measures. Additionally, it highlights the essential roles of stakeholder collaboration and regulatory compliance in fortifying supply chain security. Looking forward, the paper identifies evolving cyber threats and the need for adaptive cybersecurity strategies as key challenges, calling for continued prioritization of cybersecurity by industry and academia alike.

***Keywords**: Cybersecurity, Smart Manufacturing, Supply Chains, IoT, Blockchain, Regulatory Compliance*

Date of Submission: 22-11-2024 Date of acceptance: 04-12-2024

I. Introduction

The evolution of manufacturing into the realm of "smart" processes represents a transformative shift in how products are designed, fabricated, and delivered(Esmaeilian, Behdad, & Wang, 2016; Kusiak, 2018). At the core of smart manufacturing lies the integration of advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and machine learning, alongside traditional manufacturing processes. These integrations enable the creation of highly adaptable, efficient, and interconnected supply chains capable of real-time monitoring, predictive maintenance, and autonomous decision-making. Such advancements have increased productivity and allowed for greater customization and flexibility in manufacturing operations(Abubakr et al., 2020; Ashima et al., 2021; Lins & Givigi, 2021; Wan et al., 2020).

IoT devices play a pivotal role in these smart manufacturing supply chains by collecting and exchanging data across various stages of the manufacturing process, from raw material sourcing to final product delivery. While a boon for operational efficiency, this interconnectedness introduces significant vulnerabilities and potential entry points for cyber threats(Ben-Daya, Hassini, & Bahroun, 2019; F. Tao, Qi, Liu, & Kusiak, 2018). AI and machine learning further augment these capabilities by analyzing vast amounts of data for insights, forecasting, and optimization. Yet, they also add layers of complexity to cybersecurity considerations(Wu, Yue, Jin, & Yen, 2016).

This paper aims to delve into the intersection of cybersecurity and smart manufacturing supply chains. It aims to elucidate the critical importance of cybersecurity in this highly digitized and interconnected environment. Given the reliance of smart manufacturing on digital technologies, securing these supply chains against cyber threats is paramount. This paper explores how cybersecurity measures can be enhanced to safeguard the integrity, availability, and confidentiality of data within smart manufacturing supply chains, ensuring that the benefits of these technologies can be fully realized without compromising security.

As the sophistication and integration of technologies like IoT and AI within manufacturing supply chains increase, so do the cybersecurity challenges and risks. These technologies, while transformative, expose supply chains to a myriad of cyber threats, including but not limited to data breaches, espionage, sabotage, and ransomware attacks(Abrahams et al., 2024; I. A. I. Ahmad et al., 2024; Modupe et al., 2024; Obaigbena et al., 2024). The interconnected nature of these supply chains means that a vulnerability in one segment can have cascading effects throughout the entire chain, potentially leading to significant operational disruptions, financial losses, and damage to brand reputation. Additionally, the complexity and dynamism of smart manufacturing environments can make it difficult to effectively identify and mitigate cybersecurity risks(Atadoga et al., 2024; Okoli, Obi, Adewusi, & Abrahams, 2024; Okoro, Oladeinde, Akindote, Adegbite, & Abrahams, 2023; Okoye et al., 2024). Therefore, understanding these challenges and developing robust cybersecurity measures is critical for securing smart manufacturing supply chains.

This paper will focus on identifying and discussing comprehensive cybersecurity measures that can be adopted to enhance the security of smart manufacturing supply chains. It will cover various aspects of cybersecurity, including but not limited to identifying potential cyber threats, implementing best practices in cybersecurity, deploying advanced security technologies, and the developing of a cybersecurity framework tailored for smart manufacturing. The paper will also consider the role of regulatory compliance and the importance of collaboration among key stakeholders in achieving a secure smart manufacturing environment. Through this exploration, the paper aims to contribute valuable insights and recommendations for practitioners and researchers alike, highlighting the significance of cybersecurity in the evolution of smart manufacturing supply chains.

II. The Importance of Cybersecurity in Smart Manufacturing Supply Chains

The cybersecurity landscape in smart manufacturing supply chains is a dynamic and increasingly complex domain, shaped by the rapid evolution of digital technologies and the escalating sophistication of cyber threats. In this context, the state of cybersecurity is marked by a continuous race between the development of defensive measures and the emergence of new vulnerabilities and attack vectors. Smart manufacturing ecosystems, characterized by their reliance on IoT devices, cloud computing, and AI, present unique security challenges. These systems are inherently more exposed to cyber threats due to their extensive connectivity and the vast amounts of data they generate and process(Ebirim et al., 2024; Sodiya et al., 2024; Umoga, Sodiya, Amoo, & Atadoga, 2024).

Despite growing awareness and enhanced security protocols, many smart manufacturing operations remain vulnerable to cyberattacks. This vulnerability is partly due to the heterogeneous nature of smart manufacturing environments, which often integrate legacy systems with cutting-edge technologies, creating gaps in security that attackers can exploit. Additionally, the complexity and novelty of these technologies can outpace the development and implementation of robust cybersecurity standards and practices(Azunna, 2018; Oladeinde, Hassan, Farayola, Akindote, & Adegbite, 2023; Olatoye et al., 2024; Usman et al., 2024).

2.1 Risks and Challenges

Smart manufacturing supply chains face a range of cybersecurity risks and challenges that can undermine their integrity and functionality(Shackelford, 2019; H. Tao et al., 2019; Tuptuk & Hailes, 2018):

- Data Breaches: Given the critical role of data in smart manufacturing, from operational data to intellectual property, data breaches are a significant threat. Cybercriminals can exploit vulnerabilities to steal sensitive information, leading to loss of proprietary knowledge and competitive advantage.
- Unauthorized Access: The interconnected nature of smart manufacturing environments makes them susceptible to unauthorized access. Attackers can infiltrate the network to manipulate processes, introduce defects, or halt production, potentially causing extensive financial and reputational damage.
- Ransomware Attacks: Ransomware attacks, where attackers encrypt data or systems and demand payment for their release, can cripple manufacturing operations, leading to downtime and financial losses.
- Supply Chain Interference: Cyber threats can also target the broader supply chain, including suppliers and logistics, disrupting the flow of materials and goods and impacting the overall efficiency and reliability of the supply chain.
- Insider Threats: The complexity of smart manufacturing systems can make them vulnerable to insider threats, where individuals within the organization intentionally or unintentionally compromise cybersecurity.

The integration of various technologies amplifies these risks, making it challenging to secure the supply chain comprehensively. Moreover, the pace of technological innovation often outstrips the development of security measures, leaving systems exposed to emerging threats.

2.2 Impact of Cybersecurity Failures

The potential impacts of cybersecurity failures in smart manufacturing supply chains are profound and far-reaching(Alsharif, Mishra, & AlShehri, 2022; Dent, 2021; Lusardi, Dubovoy, & Straub, 2020):

- Operational Disruption: Cyberattacks can lead to significant operational disruptions, including shutdowns of manufacturing lines, delays in production, and loss of operational data. These disruptions can have cascading effects throughout the supply chain, affecting delivery schedules, customer satisfaction, and financial performance.
- Compromise of Data Integrity: Cybersecurity breaches can compromise data integrity, with attackers altering or destroying critical data. This can lead to flawed decision-making, production of defective products, and long-term damage to a company's reputation.

- Financial Losses: The costs associated with cybersecurity breaches can be substantial, including the direct costs of responding to attacks, legal liabilities, fines for non-compliance with regulations, and indirect costs such as lost business and reduced shareholder value.
- Erosion of Trust: One of the most damaging consequences of cybersecurity failures is the erosion of trust among customers, partners, and stakeholders. Trust is a critical asset in business relationships, and once lost, it can be challenging to rebuild.

Given these potential impacts, the importance of cybersecurity in smart manufacturing supply chains cannot be overstated. Organizations must recognize these risks and implement comprehensive cybersecurity measures to protect their operations, reputation, and bottom line.

III. Cybersecurity Measures for Smart Manufacturing Supply Chains

3.1 Best Practices

Adopting a set of cybersecurity best practices is essential to fortify smart manufacturing supply chains against cyber threats. These practices serve as the foundation for a secure operational environment, addressing common vulnerabilities and enhancing overall resilience.

- **S**ecure Device Management: Implement robust security protocols for IoT devices and other connected equipment. This includes regular firmware updates, secure authentication methods, and the management of device permissions to prevent unauthorized access.
- Data Encryption: Protect data at rest and in transit using strong encryption methods. Encryption serves as a critical line of defense, ensuring that even if data is intercepted, it remains inaccessible to unauthorized parties.
- Access Control and Identity Management: Employ stringent access control measures to ensure that only authorized personnel can access sensitive systems and data. This includes the use of multi-factor authentication (MFA), role-based access control (RBAC), and the principle of least privilege (PoLP).
- Network Segmentation: Segment networks to isolate critical systems and data from the rest of the network. This reduces the attack surface and limits the potential impact of a breach.
- Regular Security Assessments: Conduct regular security and penetration testing to identify and address vulnerabilities. This proactive approach helps to anticipate and mitigate potential security issues.
- Cybersecurity Training and Awareness: Foster a culture of cybersecurity awareness within the organization. Regular training sessions can equip employees with the knowledge and skills to effectively recognize and respond to cyber threats.

3.2 Advanced Technologies

In addition to best practices, integrating advanced technologies can significantly enhance the cybersecurity posture of smart manufacturing supply chains.

- Utilize blockchain technology to create a secure and transparent data-sharing environment across the supply chain. Blockchain's immutable ledger ensures the integrity of data transactions, making it difficult for unauthorized changes to go unnoticed.
- Leverage artificial intelligence and machine learning algorithms to monitor unusual activities and potential threats in real time. AI can analyze vast amounts of data to identify patterns indicative of cyberattacks, enabling rapid response and mitigation.
- Implement automated security solutions, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS), to monitor network traffic and automatically respond to suspicious activities.
- Adopt secure cloud computing services with robust cybersecurity measures for data storage and processing. Cloud providers typically offer advanced security features that can be leveraged to protect sensitive information.

3.3 Framework for Implementation

A structured cybersecurity framework or model is crucial for systematically addressing and mitigating risks within smart manufacturing supply chains. Organizations can adopt and tailor existing standards and guidelines to their specific needs. A suggested framework might include(Adewusi et al., 2024; Daudu et al., 2024; Modupe et al., 2024; Nwokediegwu, Ibekwe, Ilojianya, Etukudoh, & Ayorinde, 2024):

- Risk Assessment: Begin with a comprehensive risk assessment to identify critical assets, vulnerabilities, and potential threat vectors. This assessment should be revisited regularly to adapt to new threats and changes in the operational environment.
- Implementation of Controls: Based on the risk assessment, implement appropriate cybersecurity controls, including both technical measures and organizational policies.
- Continuous Monitoring: Establish continuous monitoring mechanisms to detect and respond to cybersecurity events in real-time. This includes deploying network monitoring tools and establishing a security operations centre (SOC) if feasible.

- Incident Response Plan: Develop a clear and actionable incident response plan to guide the organization's response to cybersecurity incidents. This plan should include containment, eradication, recovery, and communication procedures.
- Compliance and Review: Ensure compliance with relevant cybersecurity standards and regulations, such as ISO/IEC 27001, NIST frameworks, or industry-specific guidelines. Regularly review and update cybersecurity practices and policies to align with evolving threats and technologies.

By integrating these best practices, advanced technologies, and a structured framework, smart manufacturing supply chains can significantly enhance their cybersecurity measures. This comprehensive approach not only protects against current threats but also provides a flexible foundation to adapt to future cybersecurity challenges.

IV. The Role of Collaboration and Regulation in Enhancing Cybersecurity Measures for Smart Manufacturing Supply Chains

4.1 Stakeholder Collaboration

The importance of collaboration among stakeholders—manufacturers, suppliers, cybersecurity firms, and even customers—cannot be overstated in the complex ecosystem of smart manufacturing supply chains. This collaborative approach is crucial for several reasons. Cybersecurity is a shared responsibility. Threats can emerge at any point in the supply chain, making it imperative for all parties to actively participate in securing the network. Collaboration ensures that cybersecurity measures are uniformly strong across all supply chain nodes, preventing weak links that cybercriminals could exploit.

Collaboration facilitates sharing information regarding emerging threats, vulnerabilities, and best practices. This collective intelligence can significantly enhance the ability of stakeholders to anticipate, identify, and respond to cyber threats more effectively and swiftly. By working together, stakeholders can develop integrated cybersecurity solutions that are more robust and comprehensive. Cybersecurity firms can tailor their offerings to address smart manufacturing supply chains' specific needs and challenges. At the same time, manufacturers and suppliers can provide valuable feedback to refine these solutions.

Collaboration helps build trust among stakeholders, which is essential for the effective sharing of sensitive information and for coordinating joint responses to cyber incidents. Trust also fosters a culture of transparency and accountability, further strengthening the supply chain's resilience to cyber threats(Canestraro, Pardo, Raup-Kounovsky, & Taratus, 2009; Skopik, Settanni, & Fiedler, 2016).Effective collaboration can take various forms, including industry consortia, cybersecurity information sharing platforms, joint training programs, and collaborative research and development projects. These collaborative efforts can bridge knowledge, resources, and capabilities gaps, enabling stakeholders to enhance their cybersecurity defenses collectively.

4.2 Regulatory Compliance

The role of regulations and standards in shaping cybersecurity practices within smart manufacturing supply chains is pivotal. Frameworks such as those provided by the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC) offer structured approaches to managing and mitigating cybersecurity risks.

- Guidance and Benchmarks: Regulations and standards provide valuable guidance and benchmarks for organizations, outlining best practices and the minimum requirements for cybersecurity. Compliance with these standards can help organizations protect against a broad range of cyber threats, ensuring their data and systems' confidentiality, integrity, and availability.
- Legal and Regulatory Compliance: Beyond enhancing cybersecurity, adherence to standards and regulations is often a legal requirement. Compliance demonstrates to customers, partners, and regulatory bodies that an organization is committed to cybersecurity, potentially influencing business relationships and market access.
- Challenges of Compliance: While compliance is beneficial, it can also present challenges. These include the complexity and cost of implementing the required controls, especially for small and medium-sized enterprises (SMEs) with limited resources. Additionally, the rapidly evolving nature of cyber threats can make it difficult for regulations and standards to keep pace, potentially leaving gaps in an organization's cybersecurity defenses(A. Ahmad, Desouza, Maynard, Naseer, & Baskerville, 2020; Dutta & McCrohan, 2002).

To address these challenges, regulatory bodies need to update their standards regularly and for organizations to go beyond mere compliance by adopting a proactive and adaptive approach to cybersecurity. Furthermore, regulatory frameworks should aim to be flexible enough to accommodate the diverse needs and capabilities of different organizations while still maintaining a high standard of security.

V. Conclusion and Future Directions

5.1 Summary

This paper has underscored the pivotal role of cybersecurity in fortifying smart manufacturing supply chains against a myriad of cyber threats. As these supply chains become increasingly reliant on digital technologies such as IoT, AI, and cloud computing, they become more vulnerable to cyberattacks. We highlighted the importance of adopting cybersecurity best practices, integrating advanced technologies, and implementing a structured cybersecurity framework tailored to smart manufacturing. Furthermore, collaboration among all stakeholders and adherence to regulatory standards was emphasized as essential for creating a secure and resilient digital manufacturing ecosystem.

5.2 Future Challenges

The landscape of cyber threats is expected to evolve continuously, with cybercriminals becoming more sophisticated in their methods. This evolution poses a significant challenge to the security of smart manufacturing supply chains, necessitating ongoing vigilance, research, and adaptation of cybersecurity strategies. Future areas for research may include developing more advanced AI-driven security tools, exploring quantum-resistant encryption methods, and investigating the human factors in cybersecurity to enhance overall system resilience. Additionally, as the integration of digital technologies in manufacturing processes deepens, there will be an increased need for cross-sector and interdisciplinary collaboration to address the complex challenges that arise.

Given these challenges and opportunities, we call upon industry practitioners, researchers, and policymakers to prioritize cybersecurity within smart manufacturing supply chains. It is essential to foster an environment of continuous learning and innovation, where the development and implementation of cutting-edge cybersecurity solutions are in step with the rapid advancements in manufacturing technologies. By doing so, we can ensure that the benefits of smart manufacturing are fully realized without compromising the security and integrity of these critical systems. Let us commit to a future where smart manufacturing thrives on the foundations of robust cybersecurity, ensuring sustainable growth and resilience in the face of evolving cyber threats.

References

[1]. Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. Computer Science & IT Research Journal, 5(1), 100-119.

[2]. Abubakr, M., Abbas, A. T., Tomaz, I., Soliman, M. S., Luqman, M., & Hegab, H. (2020). Sustainable and smart manufacturing: an integrated approach. Sustainability, 12(6), 2280.

[3]. Adewusi, A. O., Asuzu, O. F., Olorunsogo, T., Iwuanyanwu, C., Adaga, E., & Daraojimba, D. O. (2024). AI in precision agriculture: A review of technologies for sustainable farming practices.

[4]. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), 939-953.

[5]. Ahmad, I. A. I., Anyanwu, A. C., Onwusinkwue, S., Dawodu, S. O., Akagha, O. V., & Ejairu, E. (2024). Cybersecurity challenges in smart cities: A case review of african metropolises. Computer Science & IT Research Journal, 5(2), 254-269.

[6]. Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science & Engineering, 40(3).

[7]. Ashima, R., Haleem, A., Bahl, S., Javaid, M., Mahla, S. K., & Singh, S. (2021). Automation and manufacturing of smart materials in Additive Manufacturing technologies using Internet of Things towards the adoption of Industry 4.0. Materials Today: Proceedings, 45, 5081-5088.

[8]. Atadoga, A., Awonuga, K. F., Ibeh, C. V., Ike, C. U., Olu-lawal, K. A., & Usman, F. O. (2024). Harnessing data analytics for sustainable business growth in the us renewable energy sector. Engineering Science & Technology Journal, 5(2), 460-470.

[9]. Azunna, C. (2018). Post-colonial agricultural participat ion in livelihood strengthening. Research, Society and Development, 7(2), 772144.

[10]. Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: a literature review. International Journal of Production Research, 57(15-16), 4719-4742.

[11]. Canestraro, D. S., Pardo, T. A., Raup-Kounovsky, A. N., & Taratus, D. (2009). Regional telecommunication incident coordination: Sharing information for rapid response. Information Polity, 14(1-2), 113-126.

[12]. Daudu, C. D., Adefemi, A., Adekoya, O. O., Okoli, C. E., Ayorinde, O. B., & Daraojimba, A. I. (2024). Lng and climate change: Evaluating its carbon footprint in comparison to other fossil fuels. Engineering Science & Technology Journal, 5(2), 412-426.

[13]. Dent, P. (2021). Cybersecurity Failures of Small and Medium-Sized Businesses: Circumventing Leadership Failure. Utica College,

[14]. Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67-87.

[15]. Ebirim, G. U., Odonkor, B., Oshioste, E. E., Awonuga, K. F., Ndubuisi, N. L., Adelekan, O. A., & Unigwe, I. F. (2024). Evolving trends in corporate auditing: A systematic review of practices and regulations in the United States.

[16]. Esmaeilian, B., Behdad, S., & Wang, B. (2016). The evolution and future of manufacturing: A review. Journal of manufacturing systems, 39, 79-100.

[17]. Kusiak, A. (2018). Smart manufacturing. International Journal of Production Research, 56(1-2), 508-517.

[18]. Lins, R. G., & Givigi, S. N. (2021). Cooperative robotics and machine learning for smart manufacturing: platform design and trends within the context of industrial internet of things. IEEE Access, 9, 95444-95455.

[19]. Lusardi, M. C., Dubovoy, I., & Straub, J. (2020). Determining the Impact of Cybersecurity Failures During and Attributable to Pandemics and Other Emergency Situations. Paper presented at the 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR).

[20]. Modupe, O. T., Otitoola, A. A., Oladapo, O. J., Abiona, O. O., Oyeniran, O. C., Adewusi, A. O., . . . Obijuru, A. (2024). Reviewing the transformational impact of edge computing on real-time data processing and analytics. Computer Science & IT Research Journal, 5(3), 693-702.

[21]. Nwokediegwu, Z. Q. S., Ibekwe, K. I., Ilojianya, V. I., Etukudoh, E. A., & Ayorinde, O. B. (2024). Renewable energy technologies in engineering: A review of current developments and future prospects. Engineering Science & Technology Journal, 5(2), 367-384.

[22]. Obaigbena, A., Lottu, O. A., Ugwuanyi, E. D., Jacks, B. S., Sodiya, E. O., & Daraojimba, O. D. (2024). AI and human-robot interaction: A review of recent advances and challenges. GSC Advanced Research and Reviews, 18(2), 321-330.

[23]. Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms.

[24]. Okoro, Y. O., Oladeinde, M., Akindote, O. J., Adegbite, A. O., & Abrahams, T. O. (2023). Digital communication and us economic growth: A comprehensive exploration of technology's impact on economic advancement. Computer Science & IT Research Journal, 4(3), 351-367.

[25]. Okoye, C. C., Ofodile, O. C., Tula, S. T., Nifise, A. O. A., Falaiye, T., Ejairu, E., & Addy, W. A. (2024). Risk management in international supply chains: A review with USA and African Cases. Magna Scientia Advanced Research and Reviews, 10(1), 256-264.

[26]. Oladeinde, M., Hassan, A. O., Farayola, O. A., Akindote, O. J., & Adegbite, A. O. (2023). Review of it innovations, data analytics, and governance in nigerian enterprises. Computer Science & IT Research Journal, 4(3), 300-326.

[27]. Olatoye, F. O., Awonuga, K. F., Mhlongo, N. Z., Ibeh, C. V., Elufioye, O. A., & Ndubuisi, N. L. (2024). AI and ethics in business: A comprehensive review of responsible AI practices and corporate responsibility. International Journal of Science and Research Archive, 11(1), 1433-1443.

[28]. Shackelford, S. J. (2019). Smart factories, dumb policy? Managing cybersecurity and data privacy risks in the industrial internet of things. Minn. JL Sci. & Tech., 21, 1.

[29]. Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154-176.

[30]. Sodiya, E. O., Jacks, B. S., Ugwuanyi, E. D., Adeyinka, M. A., Umoga, U. J., Daraojimba, A. I., & Lottu, O. A. (2024). Reviewing the role of AI and machine learning in supply chain analytics. GSC Advanced Research and Reviews, 18(2), 312-320.

[31]. Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. Journal of manufacturing systems, 48, 157-169.

[32]. Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. Future Generation Computer Systems, 98, 660-671.

[33]. Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. Journal of manufacturing systems, 47, 93-106.

[34]. Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. International Journal of Science and Research Archive, 11(1), 1810-1817.

[35]. Usman, F. O., Eyo-Udo, N. L., Etukudoh, E. A., Odonkor, B., Ibeh, C. V., & Adegbola, A. (2024). A critical review of ai-driven strategies for entrepreneurial success. International Journal of Management & Entrepreneurship Research, 6(1), 200-215.

[36]. Wan, J., Li, X., Dai, H.-N., Kusiak, A., Martinez-Garcia, M., & Li, D. (2020). Artificial-intelligence-driven customized manufacturing factory: key technologies, applications, and challenges. Proceedings of the IEEE, 109(4), 377-398.

[37]. Wu, L., Yue, X., Jin, A., & Yen, D. C. (2016). Smart supply chain management: a review and implications for future research. The international journal of logistics management, 27(2), 395-417.