IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Mitigating Cyber Risks in Supply Chain Operations: A Security-Centric Approach

Ramya Vani Rayala[1] and Sireesha Kolla[2]
Health Care Service Corporation[1]
National Institutes of Health[2]
ramyavanirayala@gmail.com and siri.kolla@gmail.com
ORCID- 0009-0002-8930-9575 and ORCID: 0009-0009-9956-2559

Abstract: *Cybersecurity in the supply chain has become a very big deal in the modern business world. Globalization is at the center of the supply chains that are joined by a variety of industries. Consequently, cybercriminals are more often exploiting the vulnerabilities in these networks. The collaboration of various stakeholders, such as suppliers, manufacturers, and logistics providers, also creates a massive number of access points for the evildoers to exploit. This paper would explore the different cybersecurity risks experienced in supply chain operations and put forward some effective plans for diminishing these threats. The study considers the ways in which supply chain resilience, security frameworks, and technology-driven solutions contribute to a multilayered approach applicable in the supply chain protection. The paper also focuses on the organizational culture, collaborations among stakeholders, and compliance to global standards that can keep the supply chain systems intact and secure.*

Keywords: Cybersecurity, Risk Mitigation, Supply Chain, Operations, Threats, Resilience, Security Framework, Global Standards

I. INTRODUCTION

The globalization of supply chains has led to increased efficiency, cost reduction, and greater market reach for organizations, but it has also introduced significant cybersecurity risks[1]. The complexity of modern supply chains, which involve multiple third-party vendors, cross-border logistics, and digital transactions, increases the attack surface for cybercriminals. The rapid advancement of digital technologies such as cloud computing, Internet of Things (IoT), and artificial intelligence (AI) has further expanded the potential vulnerabilities within supply chains. Cyberattacks on supply chains can lead to significant disruptions, financial losses, and damage to brand reputation. Thus, it is essential to adopt a robust cybersecurity framework to protect supply chain operations from emerging threats. Historically, supply chain cybersecurity has often been overlooked, with organizations focusing more on physical security and operational efficiency. However, the rise in cyberattacks targeting supply chain networks has made cybersecurity an indispensable part of risk management[2]. Incidents such as the NotPetya ransomware attack, which crippled global supply chains, have highlighted the devastating impact of cyber threats. The digital transformation of supply chains, while enhancing operational efficiency, has exposed organizations to new risks, particularly when third-party vendors fail to adhere to robust cybersecurity protocols. This has forced organizations to rethink their approach to securing their supply chains. Moreover, supply chain cybersecurity is not limited to large organizations. Small and medium-sized enterprises (SMEs), which form a critical part of many supply chains, are also vulnerable to cyberattacks. SMEs often lack the resources and expertise to implement effective cybersecurity measures, making them attractive targets for cybercriminals. The interconnected nature of supply chains means that a security breach at a small vendor can have far-reaching consequences for the entire network. Therefore, cybersecurity in supply chains must be a collaborative effort involving all stakeholders, regardless of their size or role. The growing reliance on digital technologies and third-party vendors has also increased the complexity of supply chain cybersecurity. Traditional security measures, such as firewalls and antivirus software, are no longer sufficient to protect against sophisticated cyber threats. Organizations

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 9, June 2025 Impact Factor: 7.67

must adopt a proactive approach to cybersecurity, which includes continuous monitoring, threat intelligence sharing, and incident response planning. This requires a shift in mindset from reactive to proactive risk management, with an emphasis on preventing cyberattacks before they occur [3].

The need for effective supply chain cybersecurity is further underscored by regulatory requirements and industry standards. Governments and industry bodies have introduced regulations to ensure the security of supply chains, particularly in critical sectors such as healthcare, defense, and energy. Compliance with these regulations is not only a legal obligation but also a business imperative, as failure to meet cybersecurity standards can result in penalties, reputational damage, and loss of business opportunities[4]. cybersecurity is no longer an optional consideration for supply chain operations. It is a critical component of risk management that must be integrated into every aspect of supply chain management. By adopting a comprehensive cybersecurity strategy, organizations can protect their supply chains from emerging threats, ensure business continuity, and maintain their competitive advantage in the global market.

Cybersecurity Threats in Supply Chain Operations:

Supply chains face a myriad of cybersecurity threats, ranging from ransomware and data breaches to sophisticated attacks such as advanced persistent threats (APTs)[5]. These threats can originate from various sources, including nation-state actors, cybercriminal organizations, and insider threats. The complexity of modern supply chains, with their reliance on third-party vendors and digital technologies, increases the risk of cyberattacks, as malicious actors can exploit vulnerabilities at any point in the supply chain. One of the most prevalent cybersecurity threats in supply chains is ransomware. Cybercriminals use ransomware to encrypt critical data and demand payment for its release. In a supply chain context, ransomware can disrupt the flow of goods and services, causing delays and financial losses. For example, the NotPetya attack, which initially targeted a Ukrainian software company, quickly spread across global supply chains, affecting major corporations such as Maersk and FedEx. The attack caused billions of dollars in damages and highlighted the vulnerability of supply chains to ransomware. Data breaches are another significant cybersecurity threat in supply chains [6]. Supply chains often handle sensitive information, including intellectual property, customer data, and financial records. Cybercriminals can target this information for financial gain or espionage purposes. A data breach in a supply chain can have far-reaching consequences, including regulatory penalties, loss of customer trust, and damage to brand reputation. In addition, supply chain networks often involve the sharing of sensitive data between multiple parties, increasing the risk of data leakage or unauthorized access.

Advanced persistent threats (APTs) pose a unique challenge to supply chain cybersecurity. APTs are highly sophisticated cyberattacks that involve prolonged and targeted efforts to infiltrate a network. In a supply chain context, APTs can be used to gain unauthorized access to critical systems, monitor communications, and exfiltrate data over an extended period. Nation-state actors and cybercriminal organizations often use APTs to target supply chains, particularly in industries such as defense, technology, and healthcare. The covert nature of APTs makes them difficult to detect, and they can cause significant damage before being discovered. Insider threats also represent a major cybersecurity risk for supply chains. Insider threats can arise from employees, contractors, or third-party vendors who have access to critical systems and data [7]. These individuals may intentionally or unintentionally compromise the security of the supply chain. For example, an employee with malicious intent may steal sensitive information or install malware, while a careless vendor may fail to implement adequate security controls, leading to a data breach. Organizations must be vigilant in managing insider threats and ensuring that all parties in the supply chain adhere to cybersecurity best practices.

In addition to these direct threats, supply chains are also vulnerable to supply chain attacks, where cybercriminals target a supplier or vendor to gain access to the broader network. This type of attack is particularly concerning because it can bypass traditional security measures. For example, in the SolarWinds attack, cybercriminals compromised a software update from a trusted vendor, allowing them to infiltrate the networks of multiple organizations[8]. Supply chain attacks highlight the importance of vetting third-party vendors and ensuring that they adhere to robust cybersecurity standards. Finally, the increasing use of IoT devices in supply chains presents new cybersecurity challenges. IoT devices, such as sensors and tracking systems, are often used to monitor and manage supply chain operations. However,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

these devices are frequently deployed with minimal security protections, making them vulnerable to cyberattacks. A compromised IoT device can serve as an entry point for cybercriminals, allowing them to disrupt supply chain operations or steal sensitive data. Organizations must ensure that IoT devices are properly secured and regularly updated to mitigate this risk [9].

Risk Mitigation Strategies for Cybersecurity:

Mitigating cybersecurity risks in supply chain operations requires a multi-layered approach that addresses both technological and organizational vulnerabilities. One of the most effective strategies is the implementation of a comprehensive cybersecurity framework that encompasses risk assessment, monitoring, incident response, and recovery. This framework should be tailored to the specific needs and risks of the supply chain and continuously updated to address emerging threats. Risk assessment is a critical first step in mitigating cybersecurity threats in supply chains. Organizations must conduct thorough assessments to identify vulnerabilities and potential attack vectors within their supply chain networks. This includes evaluating the cybersecurity practices of third-party vendors, as well as internal systems and processes. A risk-based approach allows organizations to prioritize their cybersecurity efforts and allocate resources where they are most needed. By identifying and addressing vulnerabilities before they can be exploited, organizations can significantly reduce the likelihood of a successful cyberattacks. Once risks have been identified, continuous monitoring of supply chain networks is essential for detecting and responding to cyber threats in real-time. Advanced monitoring tools, such as intrusion detection systems (IDS) and security information and event management (SIEM) systems, can help organizations identify unusual activity and potential security incidents. In addition, organizations should establish threat intelligence sharing partnerships with other industry players and government agencies to stay informed of emerging threats. By staying ahead of cybercriminals, organizations can reduce the impact of cyberattacks on their supply chain operations.

Incident response planning is another key component of risk mitigation in supply chains. Organizations must have a well-defined incident response plan that outlines the steps to be taken in the event of a cybersecurity breach. This includes identifying key personnel, establishing communication protocols, and defining recovery procedures. A well-executed incident response plan can minimize the damage caused by a cyberattack and ensure a swift recovery of supply chain operations. In addition, organizations should regularly test their incident response plans through simulations and drills to ensure that they are prepared for a real-world cybersecurity incident. The use of encryption and secure communication protocols is essential for protecting sensitive data in supply chains. Organizations should encrypt data both at rest and in transit to prevent unauthorized access. In addition, secure communication protocols, such as virtual private networks (VPNs) and secure file transfer protocols (SFTP), should be used to ensure the integrity and confidentiality of data exchanged between supply chain partners. By implementing robust data protection measures, organizations can reduce the risk of data breaches and ensure that sensitive information remains secure. Third-party risk management is a critical aspect of supply chain cybersecurity. Organizations must carefully vet their suppliers and vendors to ensure that they adhere to strong cybersecurity practices. This includes conducting security audits, requiring compliance with industry standards, and establishing cybersecurity requirements in contracts. In addition, organizations should monitor the cybersecurity performance of their vendors on an ongoing basis to identify potential risks. By holding third-party vendors accountable for their cybersecurity practices, organizations can reduce the risk of supply chain attacks [10].

Training and awareness programs are essential for mitigating the risk of insider threats in supply chains. Employees, contractors, and vendors must be educated on cybersecurity best practices and the potential risks associated with supply chain operations. This includes training on how to recognize phishing attempts, secure passwords, and report suspicious activity. Regular training sessions and awareness campaigns can help create a culture of cybersecurity within the organization and reduce the likelihood of insider threats. Finally, organizations should consider adopting advanced technologies, such as artificial intelligence (AI) and blockchain, to enhance their cybersecurity posture. AI can be used to detect anomalies and predict potential cyberattacks, while blockchain can provide a secure and transparent record of supply chain transactions. By leveraging these emerging technologies, organizations can strengthen their defenses against cyber threats and improve the overall security of their supply chain operations [11].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

The Role of Technology in Enhancing Cybersecurity:

Technology plays a pivotal role in enhancing the cybersecurity of supply chains, offering both tools for defense and methods for ensuring transparency and accountability. One of the most significant technological advancements in this domain is artificial intelligence (AI), which has been increasingly deployed to detect and mitigate cyber threats in real time. AI-based systems are capable of analyzing vast amounts of data to identify patterns and anomalies, helping organizations detect potential cyberattacks before they can cause significant damage. By automating the threat detection process, AI reduces the time it takes to identify and respond to security incidents, which is critical in mitigating the impact of cyberattacks on supply chain operations. Machine learning, a subset of AI, has proven to be particularly useful in improving cybersecurity for supply chains. Machine learning algorithms can analyze historical data to predict potential vulnerabilities and attack vectors, allowing organizations to proactively address these risks [12]. Furthermore, machine learning models can adapt to evolving threats, ensuring that cybersecurity defenses remain effective in the face of new attack techniques. For example, machine learning can be used to enhance the accuracy of intrusion detection systems, reducing the number of false positives and allowing security teams to focus on genuine threats. Blockchain technology has also emerged as a valuable tool for enhancing supply chain cybersecurity. Blockchain's decentralized and immutable nature provides a secure and transparent way to track and verify supply chain transactions. Each transaction is recorded in a distributed ledger, which is tamper-proof and accessible to all participants in the supply chain. This creates a single source of truth that can be used to verify the authenticity and integrity of goods and data. In addition, blockchain can help prevent supply chain attacks by ensuring that only authorized parties have access to sensitive information.

Cloud computing is another technology that has significantly impacted supply chain operations. While cloud-based solutions offer numerous benefits, including scalability and cost-efficiency, they also introduce new cybersecurity risks. Organizations must ensure that their cloud environments are properly secured, using encryption, access controls, and continuous monitoring to protect sensitive data. Multi-factor authentication (MFA) and zero-trust architectures can further enhance the security of cloud-based supply chains by ensuring that only authorized users have access to critical systems and data. The Internet of Things (IoT) has revolutionized supply chain management, enabling real-time tracking and monitoring of goods, assets, and inventory. However, the widespread adoption of IoT devices has also introduced new cybersecurity challenges. IoT devices are often deployed with minimal security features, making them vulnerable to cyberattacks. To mitigate these risks, organizations must implement strong authentication mechanisms, regularly update device firmware, and segment their networks to isolate IoT devices from critical systems. Additionally, the use of AI-driven cybersecurity solutions can help detect and respond to threats targeting IoT devices in supply chain operations.

Advanced encryption techniques are essential for protecting sensitive data in supply chains. End-to-end encryption ensures that data is encrypted at every stage of the supply chain, preventing unauthorized access or tampering. Organizations should also consider using homomorphic encryption, which allows computations to be performed on encrypted data without decrypting it. This technique can be particularly useful in supply chains where sensitive data needs to be shared between multiple parties without exposing it to potential security risks. By encrypting data both at rest and in transit, organizations can ensure the confidentiality and integrity of supply chain information. In addition to these technologies, security automation tools are increasingly being used to streamline cybersecurity processes in supply chains. Automation can help reduce the burden on security teams by automatically performing routine tasks, such as patch management, vulnerability scanning, and log analysis. By automating these processes, organizations can ensure that their supply chain networks are continuously monitored and protected against potential cyber threats. Security automation also enables organizations to respond to incidents more quickly, reducing the time it takes to detect, contain, and recover from a cyberattack.

Organizational Culture and Stakeholder Collaboration:

The effectiveness of cybersecurity in supply chain operations is not only dependent on technology but also on organizational culture and collaboration among stakeholders. Establishing a culture of cybersecurity within an organization is essential for ensuring that all employees, from top management to operational staff, understand the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 9, June 2025 Impact Factor: 7.67

importance of cybersecurity and take proactive steps to protect the supply chain. A strong cybersecurity culture encourages employees to view cybersecurity as a shared responsibility and fosters a commitment to following best practices and procedures. One of the key elements of fostering a cybersecurity culture is leadership commitment. Senior management must demonstrate a clear commitment to cybersecurity by allocating the necessary resources, setting clear policies, and leading by example. When leaders prioritize cybersecurity, it sends a message to the entire organization that it is a critical business function. Leadership should also ensure that cybersecurity is integrated into the organization's overall risk management strategy and that all decisions related to supply chain operations take cybersecurity into account. In addition to leadership commitment, continuous training and education are essential for maintaining a strong cybersecurity culture. Cybersecurity threats are constantly evolving, and employees must be equipped with the knowledge and skills to recognize and respond to these threats. Regular training sessions, awareness campaigns, and phishing simulations can help employees stay informed about the latest cybersecurity risks and best practices. In addition, organizations should provide specialized training for employees who handle sensitive supply chain data or systems, ensuring that they are aware of the specific cybersecurity risks associated with their roles.

Collaboration among stakeholders is another critical factor in ensuring the cybersecurity of supply chain operations. Supply chains involve multiple parties, including suppliers, manufacturers, logistics providers, and customers, all of whom play a role in securing the network. Effective collaboration between these stakeholders is essential for identifying and mitigating cybersecurity risks. Organizations must establish clear communication channels and protocols for sharing threat intelligence, reporting incidents, and coordinating responses to cyber threats. By working together, supply chain partners can develop a unified approach to cybersecurity and enhance the overall security of the supply chain. Third-party vendors represent a significant risk in supply chain cybersecurity, as they often have access to critical systems and data. To mitigate this risk, organizations must establish strong relationships with their vendors and ensure that they adhere to cybersecurity best practices. This can be achieved through regular security audits, vendor assessments, and the inclusion of cybersecurity requirements in contracts. In addition, organizations should work with their vendors to develop incident response plans and ensure that they are prepared to respond to a cybersecurity breach [13].

Industry collaboration is also essential for improving supply chain cybersecurity. Many industries, such as healthcare, finance, and energy, have established cybersecurity information-sharing organizations (ISOs) that allow companies to share threat intelligence and best practices. Participation in these organizations can help supply chain partners stay informed about emerging threats and learn from the experiences of others. Governments and regulatory bodies also play a role in fostering collaboration by providing guidance, standards, and frameworks for supply chain cybersecurity. Finally, the importance of compliance with global cybersecurity standards cannot be overstated. Organizations must ensure that their supply chain operations comply with industry standards, such as ISO 27001, NIST Cybersecurity Framework, and GDPR, among others. Compliance not only helps protect against cyber threats but also demonstrates to customers and partners that the organization is committed to maintaining high cybersecurity standards. Regular audits and assessments can help organizations ensure that they remain in compliance with these standards and continuously improve their cybersecurity posture.

II. CONCLUSION

Cybersecurity in supply chain operations is a critical concern in today's digital age, where the interconnectedness of global networks exposes organizations to an array of sophisticated cyber threats. This paper has highlighted the key cybersecurity risks faced by supply chains, including ransomware, data breaches, advanced persistent threats, and insider threats. These vulnerabilities are exacerbated by the reliance on third-party vendors, the proliferation of IoT devices, and the use of cloud-based solutions in supply chain management. To mitigate these risks, organizations must adopt a multi-layered cybersecurity strategy that includes risk assessment, continuous monitoring, incident response planning, and third-party risk management. The role of technology, particularly AI, blockchain, and advanced encryption techniques, is essential in enhancing the cybersecurity posture of supply chains. However, technology alone is not sufficient. A strong organizational culture that prioritizes cybersecurity and fosters collaboration among supply chain stakeholders is also critical for reducing vulnerabilities and ensuring the security of supply chain operations.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

REFERENCES

[1] S. E. V. S. Pillai, R. Vallabhaneni, P. K. Pareek, and S. Dontu, "Financial Fraudulent Detection using Vortex Search Algorithm based Efficient 1DCNN Classification," in 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT), 2024: IEEE, pp. 1-6.

[2] I. Naseer, "Implementation of Hybrid Mesh firewall and its future impacts on Enhancement of cyber security," MZ Computing Journal, vol. 1, no. 2, 2020.

[3] F. Del Giorgio Solfa, "Impacts of Cyber Security and Supply Chain Risk on Digital Operations," 2022.

[4] I. Naseer, "The efficacy of Deep Learning and Artificial Intelligence framework in enhancing Cybersecurity, Challenges and Future Prospects," Innovative Computer Sciences Journal, vol. 7, no. 1, 2021.

[5] R. Vallabhaneni, S. E. V. S. Pillai, S. A. Vaddadi, S. R. Addula, and B. Ananthan, "Secured web application based on CapsuleNet and OWASP in the cloud," Indonesian Journal of Electrical Engineering and Computer Science, vol. 35, no. 3, pp. 1924-1932, 2024.

[6] S. Kumar and R. R. Mallipeddi, "Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions," Production and Operations Management, vol. 31, no. 12, pp. 4488-4500, 2022.

[7] S. Pandey, R. K. Singh, A. Gunasekaran, and A. Kaushik, "Cyber security risks in globalized supply chains: conceptual framework," Journal of Global Operations and Strategic Sourcing, vol. 13, no. 1, pp. 103-128, 2020.

[8] I. Naseer, "Machine Learning Algorithms for Predicting and Mitigating DDoS Attacks Iqra Naseer," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 22s, p. 4, 2024.

[9] N. Gupta, A. Tiwari, S. T. Bukkapatnam, and R. Karri, "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks," IEEE Access, vol. 8, pp. 47322-47333, 2020.

[10] S. Parker, Z. Wu, and P. D. Christofides, "Cybersecurity in process control, operations, and supply chain," Computers & Chemical Engineering, vol. 171, p. 108169, 2023.

[11] H. Boyes, "Cybersecurity and cyber-resilient supply chains," Technology Innovation Management Review, vol. 5, no. 4, p. 28, 2015.

[12] S. A. Melnyk, T. Schoenherr, C. Speier-Pero, C. Peters, J. F. Chang, and D. Friday, "New challenges in supply chain management: cybersecurity across the supply chain," International Journal of Production Research, vol. 60, no. 1, pp. 162-183, 2022.

[13] F. C. Boyd, "The Effectiveness of Federal Policy in the Identification and Mitigation of Cybersecurity Supply Chain Threats," Utica College, 2020.

[14] Vallabhaneni, R., Vaddadi, S. A., Pillai, S. E. V. S., Addula, S. R., & Ananthan, B. (2024). Detection of cyberattacks using bidirectional generative adversarial network. Indonesian Journal of Electrical Engineering and Computer Science, 35(3), 1653-1660.

[15] Vallabhaneni, R., Vaddadi, S. A., Pillai, S. E. V. S., Addula, S. R., & Ananthan, B. (2024). MobileNet based secured compliance through open web application security projects in cloud system. Indonesian Journal of Electrical Engineering and Computer Science, 35(3), 1661-1669.

[16] Vaddadi, S. A., Vallabhaneni, R., & Whig, P. (2023). Utilizing AI and machine learning in cybersecurity for sustainable development through enhanced threat detection and mitigation. International Journal of Sustainable Development Through AI, ML and IoT, 2(2), 1-8.

[17] Vallabhaneni, R. (2024). Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices. Engineering And Technology Journal, 9(7), 4439-4442.

[18] Pillai, S. E. V. S., Vallabhaneni, R., Pareek, P. K., & Dontu, S. (2024, March). The People Moods Analysing Using Tweets Data on Primary Things with the Help of Advanced Techniques. In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT) (pp. 1-6). IEEE.

[19] Pansara, R. R., Vaddadi, S. A., Vallabhaneni, R., Alam, N., Khosla, B. Y., & Whig, P. (2024, February). Fortifying Data Integrity using Holistic Approach to Master Data Management and Cybersecurity Safeguarding. In 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1424-1428). IEEE.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 9, June 2025 Impact Factor: 7.67

[20] Pillai, S. E. V. S., Vallabhaneni, R., Pareek, P. K., & Dontu, S. (2024, March). Strengthening Cybersecurity using a Hybrid Classification Model with SCO Optimization for Enhanced Network Intrusion Detection System. In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT) (pp. 1-9). IEEE.

[21] Vallabhaneni, R. (2024). Evaluating Transferability of Attacks across Generative Models.

[22] Vallabhaneni, R., Nagamani, H. S., Harshitha, P., & Sumanth, S. (2024, March). Team Work Optimizer Based Bidirectional LSTM Model for Designing a Secure Cybersecurity Model. In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT) (pp. 1-6). IEEE.

[23] Vallabhaneni, R., Nagamani, H. S., Harshitha, P., & Sumanth, S. (2024, March). Feature Selection Using COA with Modified Feedforward Neural Network for Prediction of Attacks in Cyber-Security. In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT) (pp. 1-6). IEEE.

[24] Vallabhaneni, R., Nagamani, H. S., Harshitha, P., & Sumanth, S. (2024, March). Protecting the Cybersecurity Network Using Lotus Effect Optimization Algorithm Based SDL Model. In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT) (pp. 1-7). IEEE.

[25] Vallabhaneni, R., Vaddadi, S. A., Maroju, A., & Dontu, S. (2023). An Intrusion Detection System (Ids) Schemes for Cybersecurity in Software Defined Networks.

[26] Vallabhaneni, R., AbhilashVaddadi, S. A., & Dontu, S. (2023). An Empirical Paradigm on Cybersecurity Vulnerability Mitigation Framework.

[27] Vallabhaneni, R., Pillai, S. E. V. S., Vaddadi, S. A., Addula, S. R., & Ananthan, B. (2024). Optimized deep neural network based vulnerability detection enabled secured testing for cloud SaaS. Indonesian Journal of Electrical Engineering and Computer Science, 36(3), 1950-1959.

[28] Vaddadi, S. A., Pillai, S. E. V. S., Addula, S. R., Vallabhaneni, R., & Ananthan, B. (2024). An efficient convolutional neural network for adversarial training against adversarial attack. Indonesian Journal of Electrical Engineering and Computer Science, 36(3), 1769-1777.

[29] Meesala, M. K., Vallabhaneni, R., Mathapati, M., Pareek, P. K., & Metan, J. (2024, September). Arithmetic Optimized Bi-GRU: A Swift Approach to Combat Fake News in the Digital Sphere. In 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC) (pp. 1-6). IEEE.

[30] Dontu, S., Vallabhaneni, R., Addula, S. R., Pareek, P. K., & Hussein, R. R. (2024, August). Enhanced adaptive butterfly optimizer based feature selection for protecting the data in industry based WSN. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[31] Dontu, S., Vallabhaneni, R., Addula, S. R., Pareek, P. K., & Abbas, H. M. (2024, August). MCWOA based Hybrid Deep Learning for Detecting the Attacks in Cybersecurity with IoT Network. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-7). IEEE.

[32] Vaddadi, S. A., Pillai, S. E. V. S., Vallabhaneni, R., Addula, S. R., & Ananthan, B. (2025). Vulnerability detection in smart contact using chaos optimization-based DL model. Indonesian Journal of Electrical Engineering and Computer Science, 38(3), 1793-1803.

[33] Pillai, S. E. V. S., Vaddadi, S. A., Vallabhaneni, R., Addula, S. R., & Ananthan, B. (2025). TextBugger: an extended adversarial text attack on NLP-based text classification model. Indonesian Journal of Electrical Engineering and Computer Science, 38(3), 1735-1744.

[34] Pillai, S. E. V. S., Vallabhaneni, R., Vaddadi, S. A., Addula, S. R., & Ananthan, B. (2025). Automated adversarial detection in mobile apps using API calls and permissions. Indonesian Journal of Electrical Engineering and Computer Science, 37(3), 1672-1681.

[35] Pillai, S. E. V. S., Vallabhaneni, R., Vaddadi, S. A., Addula, S. R., & Ananthan, B. (2025). Archimedes assisted LSTM model for blockchain based privacy preserving IoT with smart cities. Indonesian Journal of Electrical Engineering and Computer Science, 37(1), 488-497.

[36] Meesala, M. K., Vallabhaneni, R., Mathapati, M., Pareek, P. K., & Metan, J. (2024, September). Beyond the Horizon: Drone-Assisted HAR Through Cutting-Edge Caps Net and Optimization Techniques. In 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC) (pp. 1-6). IEEE.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

[37] Dontu, S., Addula, S. R., Pareek, P. K., Vallabhaneni, R., & Fallah, M. H. (2024, August). A Feature Selection based Decisive Red Fox Algorithm with Deep Learning for Protecting Cybersecurity Network. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-7). IEEE.

[38] Vaddadi, S. A., Vallabhaneni, R., Maroju, A., & Dontu, S. Analysis on Security Vulnerabilities of the Modern Internet of Things (IOT) Systems.