UDK 663.576

SYSTEM SAFETY: CHALLENGES AND SOLUTIONS

Nurakov Serik Nurakovih, Kuzenbayev Iskander
kuzenbaev@gmail.com
Doctor of Technical Sciences, Professor of the department "Organization of transportation, traffic and operation of transport" L.N.Gumilyov ENU, Astana, Kazakhstan
Master's student of the department "Organization of transportation, traffic and operation of transport" L.N.Gumilyov ENU, Astana, Kazakhstan

Keywords: Logistic System Safety Cybersecurity in Logistics Risk Mitigation Strategies Emerging Technologies in Supply Chain Security

Abstract. This research, situated within the domain of Computer Science and Engineering (CSE), undertakes an exploration of Logistic System Safety. The core objective is to scrutinize challenges inherent in ensuring the safety of logistic systems and propose viable solutions. The study draws on a comprehensive review of literature from diverse sources, including Akdeniz Library, IEEE Explore, and Google Scholar, identifying prevalent threats and investigating methodologies and technologies currently applied in the field. The proposed approach involves a systematic analysis to identify challenges affecting logistic system safety, followed by a critical assessment of existing methodologies and technologies. Furthermore, the study explores emerging technologies and inventive methodologies that have the potential to elevate safety standards in logistic systems. This research holds significance in contributing valuable insights to enhance the safety of logistic systems, a critical aspect of contemporary business operations. By delineating challenges and proposing effective solutions, the study aims to establish a foundation for subsequent advancements in the field of Logistic System Safety within the realm of Computer Science and Engineering. The forthcoming paper will offer a comprehensive overview of challenges, coupled with a critical evaluation of existing solutions and introduce potential innovative approaches for further exploration.

Introduction. Navigating the intricacies of modern commerce, the operational efficiency of logistic systems emerges as a linchpin for the success of contemporary business endeavors. These systems, serving as the lifeblood of supply chains, facilitate the seamless movement of goods, demanding an unparalleled level of precision and reliability. However, the escalating integration of technology in logistics has brought forth a host of challenges, particularly in the realm of cybersecurity. This article, penned within the framework of my Computer Science and Engineering (CSE) course, embarks on a journey to delve into the critical aspect of Logistic System Safety As we set the stage, the symbiotic relationship between logistics and technology has ushered in remarkable efficiencies, yet it has concurrently unveiled a canvas of vulnerabilities. With the deepening reliance on interconnected systems, the risks to the safety and security of logistic operations become increasingly pronounced. Beyond being a technical concern, addressing these challenges becomes a strategic imperative for sustaining the integrity of modern business operations. In terms of scope and objectives, this exploration seeks to scrutinize the multifaceted challenges entwined with ensuring the safety of logistic systems. Grounded in the principles of Computer Science and Engineering, my study aims to navigate the evolving landscape of logistic operations, dissecting contemporary threats and vulnerabilities. Leveraging insights from academic databases such as Akdeniz Library, IEEE Explore, and Google Scholar, the research will undertake a comprehensive review of existing literature to identify innovative solutions capable of fortifying logistic system safety. The key research components will encompass the systematic analysis of challenges poised at the intersection of logistics and technology, a critical assessment of current methodologies and technologies deployed for ensuring logistic system safety, and the exploration of emerging technologies and inventive methodologies to enhance safety measures. Highlighting the significance of this research, it aspires to contribute to the ongoing discourse on logistic system

safety by providing valuable insights and laying a foundation for further advancements. By unraveling challenges and proposing effective solutions, the study aims to empower stakeholders in the field of Computer Science and Engineering to confidently navigate the complexities of modern logistic operations. As we embark on this academic exploration, this article endeavors to shine a light on the evolving landscape of logistic system safety. I invite the reader to join the discourse and contribute to securing the future of logistics in the ever-evolving digital era.

2. Identification of Challenges: Systematic analysis of the challenges posed to the safety of logistic systems. Digital technologies are actively implemented and evolving in the logistics sector, enabling efficient management of supply chains. Currently, they form complex networks with a vast amount of data that may be susceptible to hacker attacks. Therefore, to utilize digital technologies in logistics, due attention must be given to cybersecurity. Cybersecurity is the activity associated with protecting systems, networks, and programs from digital attacks. It is essential in logistics because data breaches can result in significant temporary and financial losses, negatively impacting company operations.

2.1. Unpacking the Cascading Consequences of Cyberattacks on Logistics and Public Safety. The importance of cybersecurity in logistics can be verified by analyzing cases where cargo transportation and storage were threatened due to cyberattacks. One such case occurred on November 16, 2020, when the major American company Americold, managing 183 warehouses, fell victim to a cyberattack. As a result of this incident, the company incurred losses as it had to temporarily shut down its information systems. The company could not manage its inventory and fulfill orders. This also affected communication through email and phone with its clients and partners. To overcome the crisis, the company collaborated with cybersecurity experts, lawyers, and law enforcement. Specialists linked the cyberattack to the refrigerated warehouses owned by Americold, where the storage of COVID-19 vaccines was planned. Andre Pienaar, who made a significant contribution to creating the Cyber Alliance to Defend Our Healthcare, consisting of 40 companies in the cybersecurity sector, commented on this incident. She mentioned that logistics companies with cold storage facilities do not invest enough in cybersecurity, making it easy for hackers to breach their systems. In September 2020, the French group of companies, CMA CGM, specializing in container shipping, also fell victim to a cyberattack. Employees, upon arriving at their workplaces and turning on their computers, encountered the following message: "Hello, if you are reading this, your data is encrypted, and your personal information is stolen." Specialists had to shut down the systems and deal with the ransomware program that infiltrated their systems. It took over a week before the company's operations returned to normal. To prevent and combat the consequences of future cyberattacks, the company hired Nicolas Sekkaki as Vice President of IT. Similar stories are frequently encountered in the news feed. The main goals of hackers usually include terrorist acts, the abduction or damage of information or digital systems that are valuable to the population, leading to people's intimidation or the risk of their death; enrichment through the sale of stolen confidential data or extortion of funds from the company. Many companies providing logistics services fall victim to cyberattacks. Their consequences may include financial losses, delivery delays, dissatisfaction among customers and partners (affecting the company's image), spoilage of stocks in warehouses, failure of information systems, leakage or destruction of confidential data and personal information of employees, and more. A cyberattack can cause harm not only to the logistics company and its clients but also to other people. For example, during the global pandemic, vaccine shipments are conducted worldwide, where temperature control is crucial. If hackers manage to take control of the system responsible for the temperature at which vaccines are transported, there is a risk of spoiling the vaccine. This will lead to many people being unable to receive it. Additionally.

Vaccines must be delivered promptly to combat COVID-19. Companies in the logistics sector need to invest in cybersecurity to prevent unauthorized access to their digital systems or mitigate the listed consequences. The report on global current cybersecurity threats by Positive Technologies indicates a rise in cyberattacks: the number of incidents in 2020 increased by 51% compared to 2019; in 86% of cases, organizations were the target of the attacks. Global transport

and logistics organizations, as well as individual countries, are concerned about the increasing number of cyberattacks and are trying to take measures to counteract them. Currently, the Russian Federation has the Federal Law dated July 26, 2017, No. 187-FZ on the security of critical information infrastructure. This law regulates relations in the field of ensuring the security of the critical information infrastructure (CII) of the Russian Federation. CII includes objects of critical information infrastructure, as well as communication networks used to organize the interaction of such objects.

2.2. The unique cybersecurity challenges of logistics operations. This research delves into the increasingly crucial domain of cybersecurity within logistics and supply chain management. While existing literature offers numerous measures for enhancing security, further exploration is needed to equip companies with comprehensive strategies against evolving cyber threats. Here's a summary of the key findings and potential research avenues:

2.2.1. Lack of Real Cybersecurity Data. Extensive theoretical frameworks dominate the research landscape, highlighting a scarcity of real-world cybersecurity data. Companies are reluctant to share information due to privacy concerns and reputational risks, hindering data acquisition for research purposes. Potential solutions include collaboration with willing companies, utilizing secondary data or simulation models, and creating hypothetical data.

2.2.2. Insufficient Studies on Logistics Cybersecurity. Research primarily focuses on supply chain management, overlooking the crucial role and unique vulnerabilities of logistics within the interconnected web. Outsourcing logistics to 3PLs creates a perception of safety, potentially masking hidden cybersecurity risks. More studies are needed to address the specific cybersecurity challenges in the logistics domain.

2.2.3. Limited Methodological Diversity. Qualitative methodologies dominate the field, reflecting the nascent stage of this research area. Growth in quantitative studies indicates emerging consensus on key concepts like cybersecurity investment and resource allocation. Further quantitative research requires readily available data on cyber network topologies, incident reports, and attack pathways.

2.2.4. Scarce Studies on Real-Time Recovery and Aftermath Measures. Most research focuses on preventative measures, neglecting crucial strategies for response and recovery when attacks occur. Optimizing real-time resource allocation for compromised components and designing resilient infrastructure could offer valuable insights. Exploring gametheoretic approaches to model attacker-defender interactions for dynamic resource allocation during ongoing attacks holds promise.

2.2.5. Blockchain's Potential and Remaining Hurdles. Blockchain's features like anonymity, distributed control, and immutability make it attractive for authentication and data protection. Applications include tracking product provenance, secure data sharing, and revolutionizing maritime shipping systems. Challenges like limited standardization, lack of widespread electronic data exchange, privacy concerns, and scalability need to be addressed for broader adoption.

2.2.6. Limitations of Current Encryption Schemes. Blockchain relies on one-way cryptographic functions vulnerable to potential future quantum computing advancements. Quantum cryptography and quantum internet offer potential solutions, but cost and practicality remain limitations. Research on quantum-resistant cryptographic techniques tailored for logistics and supply chain management is vital.

2.2.7. Advocating Information Security and Digital Forensics. Increasing reliance on smart devices, RFID technologies, and Industry 4.0 advancements expands the attack surface in supply chains. Secure information sharing among supply chain partners is crucial for mitigating cyberattacks, necessitating research on blockchain and encryption applications. User-friendly digital forensic tools and streamlined implementation processes across entire supply chain networks could significantly improve cybersecurity posture. By addressing these research gaps and actively exploring innovative solutions, we can build a more secure and resilient future for the

interconnected world of logistics and supply chains. Remember, cybersecurity is not a one-time effort, but an ongoing journey of proactive defense and continuous adaptation.

3. Securing the Supply Chain: A Critical Assessment of Cybersecurity in Logistics. The efficient flow of goods in today's interconnected world hinges on robust logistics systems. Yet, lurking beneath the surface of optimized routes and seamless deliveries lies a growing threat: cyberattacks. The security of these systems directly impacts the confidentiality, integrity, and availability of sensitive data, making comprehensive cybersecurity measures paramount. Traditional approaches have relied on employee training, IT security specialists, and basic protection systems like antivirus software and firewalls. While these remain important, their effectiveness wanes against increasingly sophisticated cyber threats. New avenues require exploration. Implementing advanced technologies like data leak prevention systems and establishing dedicated cyber information processing centers can provide real-time protection and rapid response capabilities. Additionally, staying abreast of software updates and adopting emerging security solutions is crucial to staying ahead of the curve. However, technology alone is not enough. A critical gap lies in the underrepresentation of cybersecurity professionals within logistics companies, particularly smaller ones. Addressing this through competitive salaries and targeted workforce development programs is essential. The consequences of neglecting cybersecurity are severe. From data breaches and financial losses to operational disruptions and reputational damage, the potential fallout is far-reaching. Investing in robust security measures is not just a prudent precaution, but a strategic necessity for long-term success in the logistics industry. Therefore, a multi-pronged approach is vital. Companies must:

3.1 Training of all company employees in cybersecurity. Employees should be attentive to information transmission, avoid losing various data storage devices (documents, work laptops, phones, etc.), and recognize phishing. Phishing is an attack carried out by cybercriminals through mass distribution of similar or identical content messages, including malicious attachments or links redirecting to a malicious website.

3.2 Presence of qualified digital security specialists in the staff: Currently, companies providing logistics services rarely employ such personnel. Moreover, there is a shortage of professionals in the field of cybersecurity in the labor market, as it is a relatively new direction that has been around for about 10 years. Graduates in this field rarely choose to work in the logistics sector, as many logistics companies allocate a limited budget for cybersecurity. Offering higher salaries to such specialists is necessary to draw attention to the transportation sector. Underestimating this measure can lead to the company losing control over its information systems.

3.3 Utilization of new technologies: It is essential to keep track of software updates, as outdated technologies had effective protection against threats at the time of their creation.

3.4 Use of various defense systems: To combat external threats, antivirus programs, DDoS attack detection systems, and network security screens are implemented. Antivirus programs can identify infected files and eliminate the virus code from them or, if impossible, delete the infected file entirely. DDoS attack is a distributed denial-of-service attack directed at causing a service disruption. It is crucial to detect it in a timely manner and take necessary countermeasures. Network security screens are designed to block unwanted traffic, protecting internal or trusted networks from external and untrusted ones. In most cases, it is necessary to have security systems that prevent the leakage of confidential information from the company's internal environment. An example of such a tool is the "Data Leak Prevention System." These systems will alert in case of employees transferring sensitive information outside the company. This tool also allows structuring and systematizing data and archiving operations related to the movement of information through the organization's digital technologies.

3.5 Establishment of a cyber information processing center within the company: Proprietary centers, including IT specialists, modern equipment, a budget, and a specific structure, will help react more promptly to cyber threats. This measure is relevant for large companies dealing with a significant volume of data. First and foremost, companies that have not previously paid attention to cybersecurity need to conduct a comprehensive IT audit and perform penetration testing

to identify malicious programs in the system. Penetration testing is carried out by simulating the actions of a criminal. In transportation and logistics, there are both large and small companies, and currently, there are differences in their approach to cybersecurity. Large companies are more involved in implementing protection measures and hiring qualified IT security specialists. This is because they process a lot of data and have a large number of information transmission channels. However, the increasing trend of cyberattacks also poses a threat to small companies. They are less prepared to deal with this problem. Cybersecurity is an important component of a logistics company, as ignoring this area can lead to leakage of confidential information, loss of funds (due to theft or extortion), destruction or falsification of data, as well as loss of control or malfunction of systems. The logistics company chooses whether to save on cybersecurity or not, but it needs to understand that losses in the event of a cyberattack can be many times greater.

4. Exploration of Emerging Technologies for Enhanced Logistic System Safety. The final phase of our research delves into the realm of innovation, seeking to identify and evaluate emerging technologies and inventive approaches capable of elevating the safety standards of logistic systems. In this phase, we not only look at theoretical applications but also assess the practical feasibility and scalability of these technologies in real-world logistic scenarios. We explore the integration of artificial intelligence (AI) to enhance predictive analytics and risk assessment in logistic operations. AI algorithms can analyze vast datasets, identify patterns, and predict potential safety risks, enabling proactive measures to be taken. Leveraging machine learning (ML) algorithms for anomaly detection can significantly contribute to identifying irregularities and potential security breaches in logistic processes. This innovative approach aims to enhance the system's ability to adapt and respond to evolving threats. The exploration of blockchain focuses on its application to enhance transparency and traceability in the supply chain. By creating an immutable and decentralized ledger, we aim to mitigate the risk of tampering and unauthorized access in logistic data. We investigate the integration of Internet of Things (IoT) devices to provide real-time monitoring and tracking of logistic assets. This includes sensors and connected devices to ensure the integrity and security of shipments throughout the supply chain. Additionally, we explore the use of Robotic Process Automation (RPA) in automating security protocols and response mechanisms. This involves developing robotic systems capable of swiftly identifying and neutralizing potential threats in logistic operations. By embracing these innovative approaches, our research aims to contribute forward-thinking solutions to bolster the safety of logistic systems. The synergy of these technologies presents an opportunity to not only address current challenges but also proactively prepare logistic operations for the dynamic technological landscape of the future. Through this exploration, we strive to pave the way for resilient and adaptive logistic safety mechanisms.

5. Conclusion

The intricate web of logistics systems pulsates with the very lifeblood of modern commerce. This research has embarked on a critical journey, traversing the crossroads of operational efficiency and cybersecurity within this domain. It has shed light on the multifaceted challenges posed by the evolving digital landscape, where vulnerabilities lurk beneath the surface of seamless deliveries and optimized routes. The consequences of neglecting cybersecurity in logistics are stark. From data breaches and financial losses to operational disruptions and reputational damage, the potential fallout is far-reaching. This research serves as a stark reminder that investing in robust safety measures is not a luxury, but a strategic imperative for long-term success in the logistics industry. The proposed multi-pronged approach tackles the problem head-on: Enhanced Awareness and Training: Equipping all personnel with cybersecurity knowledge and vigilance against phishing attempts is crucial. Specialized Workforce: Integrating dedicated cybersecurity professionals within logistics companies, particularly smaller ones, requires competitive salaries and targeted workforce development programs. Technological Embracing: Utilizing advanced technologies like data leak prevention systems, cyber information processing centers, and staying abreast of software updates are essential to stay ahead of the curve. Emerging Technologies: Exploring the integration of AI, ML, blockchain, IoT, and RPA presents transformative opportunities for proactive risk assessment,

anomaly detection, transparent data management, real-time monitoring, and automated security responses. This research acknowledges that large and small logistics companies operate in a diverse landscape. While large companies hold inherent advantages in implementing such measures, the increasing trend of cyberattacks makes vulnerability ubiquitous. The choice to prioritize cybersecurity is not an option, but a necessity. Our exploration ultimately strives to pave the way for a future where logistic systems are not only efficient but also resilient and adaptive. By embracing innovative approaches and prioritizing safety measures, we can ensure that the lifeblood of modern commerce continues to flow seamlessly, protected from the ever-evolving threats of the digital age. Let us navigate the crossroads of efficiency and security with foresight and responsibility, building a secure and resilient future for the global logistics ecosystem. Remember, the journey towards robust logistic system safety is not a destination, but an ongoing voyage of proactive defense and continuous adaptation. By diligently navigating the ever-changing landscape, we can ensure that the pulse of global commerce continues to beat, secure and steady, for generations to come.

References

1. References Afanasenko, I., Borisova, V., 2019. Digital logistics , 269.
2. Ajakwe, S.O., Kim, D.S., Lee, J.M., 2023. Drone transportation system: Systematic review of security dynamics for smart mobility. IEEE Internet of Things Journal 10, 14462–14482. doi:10.1109/JIOT.2023. 3266843.
3. Alekseev, A., Kuznetsova, A., Semenova, A., 2023. Logistics service quality assessment based on the system approach. Journal of Management and Business Administration 10, 10–20. doi:10.24411/ 2587-6537-2023-10010.
4. Arustamova, E.A., Pyastolav, O.A., Samoletov, R.V., et al., 2022. Ensuring the security of international trade based on digital logistics in the context of a pandemic. Actual Problems of Security: A Collection of Scientific Articles , 65–78.
5. Burrell, D., Bhargava, N., Bradley-Swanson, O., Harmon, M., Wright, J., Springs, D., Dawson, M., 2020. Supply chain and logistics management and an open door policy concerning cyber security introduction. International Journal of Management and Sustainability 9, 1–10. doi:10.18488/ journal.11.2020.91.1.10.
6. Citadel, C., 2023. The threat to the logistics industry. URL: https://www. cybercitadel. com/ resources/whitepapers/ the-threat-to-the-logistics-industry/.
7. Myasnikova, O.V., 2022. Strategy and tactics of digital transformation of production and logistics systems. Social Innovations and Social Sciences 2022, 39–49. doi:10.22394/2071-1385-2022-1-39-49.
8. Technologies, P., 2020. Cybersecurity threatscape: 2020 review. URL: https://www. ptsecurity. com/research/analytics/ cybersecurity-threatscape-2020.
9. Tenevyy, O., 2016. Methodology and Means of Early Detection and Counteraction to Threats to Information Security in DDoS Attacks. Ph.D. thesis. Tomsk State University of Control Systems and Radioelectronics. Barnaul.
10. Wang, S., Guan, Y., Xu, Z., Zhan, S., 2019. Optimization of resources for logistics safety emergency management based on maximum entropy. Entropy 21, 558. doi:10.3390/e21060558.
11. Winkelhaus, S., Grosse, E.H., 2020. Logistics 4.0: a systematic review towards a new logistics system. International Journal of Production Research 58, 18–43. URL: https://doi.org/10.1080/00207543.2019.1612964, doi:10.1080/00207543.2019.1612964,arXiv:https://doi.org/10.1080/00207543.2019.1612964.
12. Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M., 2020. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems 77, 103201. URL: https://www.sciencedirect.com/science/article/pii/S0141933120303689, doi:https://doi.org/10.1016/j.micpro.2020.103201.