Article

Not peer-reviewed version

Secure Logistics Monitoring System Based on Wireless Sensor Network

Sidra Hameed , humaira ashraf , NZ Jhanjhi *

Posted Date: 21 December 2023

doi: 10.20944/preprints202312.1641.v1

Keywords: SCM; logistics; wireless network

Article

Secure Logistics Monitoring System Based on Wireless Sensor Network

Sidra Hameed [1], Dr. Humaira Ashraf [1] and NZ Jhanjhi [2,*]

[1] Department of Computer Science and Information Technology, International Islamic University Islamabad, Pakistan; sidra.mscs1138@iiu.edu.pk (S.H.); humaira.ashraf@iiu.edu.pk (H.A.)
[2] School of Computer Science, SCS, Taylors University, Subang Jaya, Malaysia; noorzaman.jhanjhi@taylors.edu.my
* Correspondence: noorzaman.jhanjhi@taylors.edu.my

Abstract: With the emergence of Advance Logistics, the logistics industry has witnessed significant advancements, leading to a greater reliance on intelligent technologies. These technologies play a crucial role in gathering and transmitting logistics data, but they also introduce security and privacy risks to logistics management systems. The sharing of customer-sensitive information among stakeholders for efficient operations becomes vulnerable to unauthorized access, thus compromising privacy. This, amongst others, is a critical problem that needs to be addressed. The unique features of a cryptographic hash function, including immutability, efficient verification, and anonymity, make it a transformative technology that has the potential to address the mentioned challenges in various sectors. This disruptive technology offers solutions by ensuring data integrity, enabling quick verification, and preserving privacy. The findings suggest that employing Cryptographic Hash Functions to share customer data among logistics partners offers robust protection against cyber-attacks. The proposed system guarantees asset security, and as demonstrated by the case study evaluation, exhibits strong resilience in safeguarding against various security and privacy threats. Although this study is significant, it does have limitations. One of these limitations is the considerable overlap between logistics research and supply chain management (SCM). While our focus was on logistics tasks, we did not extensively delve into the broader context of SCM.

Keywords: SCM; logistics; wireless network

1. Introduction

The ability to carry and deliver items from one location to another has made logistics a crucial component of enterprises all over the world. To monitor and secure logistics operations, a trustworthy system is essential given the rising number of security threats in the supply chain. The flexibility, cost-effectiveness, and scalability of wireless sensor networks (WSN) have made them a promising solution for safe logistics monitoring in recent years.

In the modern era, Wireless Sensor Networks (WSNs) technology has grown significantly. WSNs are widely utilized in fields like the military, business, healthcare, smart cities, and smart homes. Secure communication between the sensor nodes and the base station is necessary for all WSN applications. A WSN is a collection of affordable, low-power, tiny wireless sensors that can sense and gather information about their surroundings. WSNs can give real-time information about the whereabouts, state, and security of cargo in transit when they are deployed in a logistics environment. The utilization of this information can improve security, cut costs, and optimize logistics processes. Various threats are introduced into WSN because of adversary compromises at the sensor nodes.

However, there are several security and privacy issues that come up when using WSNs in logistics applications. The wireless nature of WSN communication channels leaves them open to

 doi:10.20944/preprints202312.1641.v1

different assaults, including jamming, node capture, and eavesdropping. Therefore, it is essential to develop a safe logistics monitoring system that can reduce these security risks and give logistics operators dependable and trustworthy information. The goal of the proposed study is to create a Secure Logistics Monitoring System based on Wireless Sensor Networks to handle the security and privacy issues that arise in logistics applications. The system will be made up of a network of sensors placed on vehicles and cargo containers that will track the position, temperature, humidity, and other environmental factors affecting the products being transported. Through a secure communication link, the gathered data will be sent to a central server, where it will be processed and analyzed to offer real-time monitoring and tracking of the items.

We will protect the communication routes between the sensors and the central server using cutting-edge cryptographic techniques to assure the system's security. To prevent unauthorized access to the system, we will also integrate secure authentication and access control systems. In addition, we will assess how resilient the system is to several security assaults, such as node compromise, denial-of-service, and jammer assaults. One of the developments in logistics is the adoption of tracking and emergency decision-making technologies. The incorporation of GIS technology into the logistics process satisfies the urgent and effective needs of contemporary logistics, aids logistics distribution businesses in making effective use of available resources and facilitates the comprehensive tracking of the logistics process by the fourth party logistics. Either a cargo owner enterprise user or a third-party logistics provider can utilize the system's services, comprehend the various statuses of the items in real time while they are in the logistics process, and complete queries and statistics through the system [19,20].

Figure 1. depicts the sensor node's internal architecture. The energy supply module, which is in charge of providing energy to the other three modules so that they can function regularly, is the most basic construction, as can be seen from the image. To configure and manage the network's nodes, the sensor network must possess a certain level of self-organization. Failures at the sensor node or failures brought on by insufficient energy are frequent in real-world scenarios. or occasionally insert some nodes artificially. To configure and manage the network's nodes, the sensor network must possess a certain level of self-organization. Failures at the sensor node or failures brought on by insufficient energy are frequent in real-world scenarios. or occasionally insert some nodes artificially.

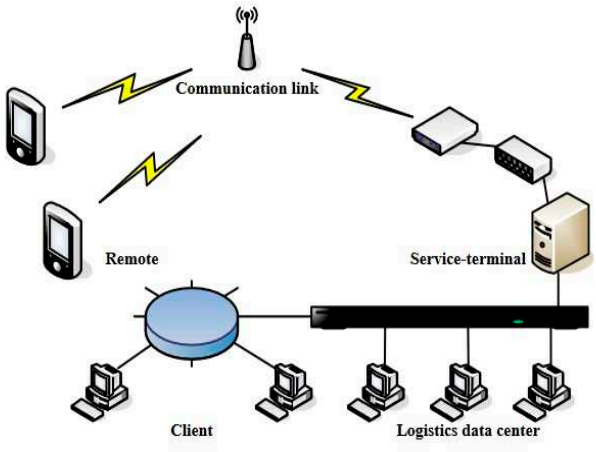

Figure 1: System framework

The Research of [1] Claims that data security and privacy are the major obstacles to deploying an IoT and cloud-based logistics system. The document could go over the system's numerous security threats, like data loss and cyber-attacks, and suggest ways to reduce those risks. For the logistics system to handle the growing user and data quantities over time, it must be dependable and scalable. To make sure the system can meet the rising needs of logistical operations, it might discuss the problems with dependability and scalability and offer alternatives. The research of [2] explains a layered security architecture strategy that incorporates security mechanisms at various IoT system tiers to improve the security of IoT systems. In the research of [3] with an emphasis on the sensors,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1641.v1

data analysis, and communication protocols employed, this paper gives a survey on various methodologies and approaches used in the development of cold storage monitoring systems using IoT. The state-of-the-art right now, as well as potential future research directions [4] it focuses on an overview of several IoT applications in the logistics business, including their advantages, difficulties, and prospective future research areas. It analyses numerous IoT technologies and their potential to improve logistics efficiency and sustainability.

There are several gaps in the present research surveys, as shown in Table 1. The surveys lack an organized presentation and comprehensive, in-depth critical and comparative analysis. the necessity of putting strong security measures in place in WSN-based logistics monitoring systems to guarantee the integrity and safety of commodities and products throughout storage and transportation. We have produced this in-depth literature evaluation to add to the field and close the gaps in the present surveys. This study presents the most recent methods and cutting-edge strategies for logistic monitoring.

Table 1. Summary of Surveys of Secure logistics monitoring system.

Years	Main Focus	Major Contribution	Developments in Our Paper
2021	Focus on develop and implement a smart and secure logistics system.	[1] the development and implementation of a smart and secure logistics system based on IoT and cloud technologies, which can optimize logistics processes and enhance supply chain security. However, it may be the need for further evaluation of the economic feasibility and cost-effectiveness of the proposed system and further investigation of the system's scalability and applicability in different logistics contexts.	Our research could evaluate the scalability of the proposed logistics system by examining its ability to handle increasing volumes of data and users
2020	Analyze the current state-of-the-art security solutions for IoT systems using a layered architecture approach.	The study of [2] is proposing a layered security architecture approach for IoT systems that integrates security mechanisms at multiple layers. The gaps identified include lack of standardized security protocols, limited attention to privacy concerns, and inadequate consideration of physical security measures.	Our survey presents proposing a layered security architecture approach for IoT systems and evaluating its potential impact on enhancing the security of IoT systems.

 doi:10.20944/preprints202312.1641.v1

2020	To review and analyze the current state-of-the-art solutions for monitoring the cold chain using IoT technologies.	The research paper [3] is to provide a comprehensive survey of the existing IoT-based solutions for cold storage monitoring, and to identify the strengths, weaknesses, opportunities, and threats of these solutions. However, it does not provide a detailed analysis of the economic feasibility and cost-effectiveness of these solutions in different practical scenarios.	Our research presents the use of temperature and humidity sensors to monitor the condition of goods during transportation, and the use of cloud-based systems for data analysis and decision-making.
2021	To provide a comprehensive review of the applications of IoT in the field of smart logistics, including the challenges, opportunities, and future directions.	The paper [4] identifies various applications of IoT in smart logistics and discusses their benefits, challenges, and future directions. However, it does not provide a detailed analysis of the technical aspects of these applications. Additionally, it does not cover some important topics such as security and privacy concerns in IoT-based smart logistics systems.	Our survey includes identifying the various applications of IoT in smart logistics, exploring the benefits and challenges of IoT in logistics, and proposing potential solutions for secure logistics monitoring based on IoT technology.

The WSN-based logistics monitoring system features real-time data gathering and analysis, as well as security measures like encryption, authentication, and data transmission protocols that use little energy [4]. The strings in the systematic literature review were created by utilizing three synonyms for each word. A search protocol was followed, and papers published in the years 2020, 2021, 2022, and 2023) were chosen for the search. Additionally, each term was searched across three databases and three synonyms. The first level of filtering is title-based, the second is abstract-based, and the third is objective-based. The first step in the filtering process was title-based filtering. Publications that failed to address the topic at hand were eliminated from the selected databases. In the second stage, abstract-based filtering was carried out. The third stage of filtering, which utilized objective-based filtering, is depicted in Figure 2. After all of the papers were sorted based on their objectives, a table displaying the papers was produced. The strategies to solve those issues were critically analyzed in the last section to determine their limitations.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1641.v1

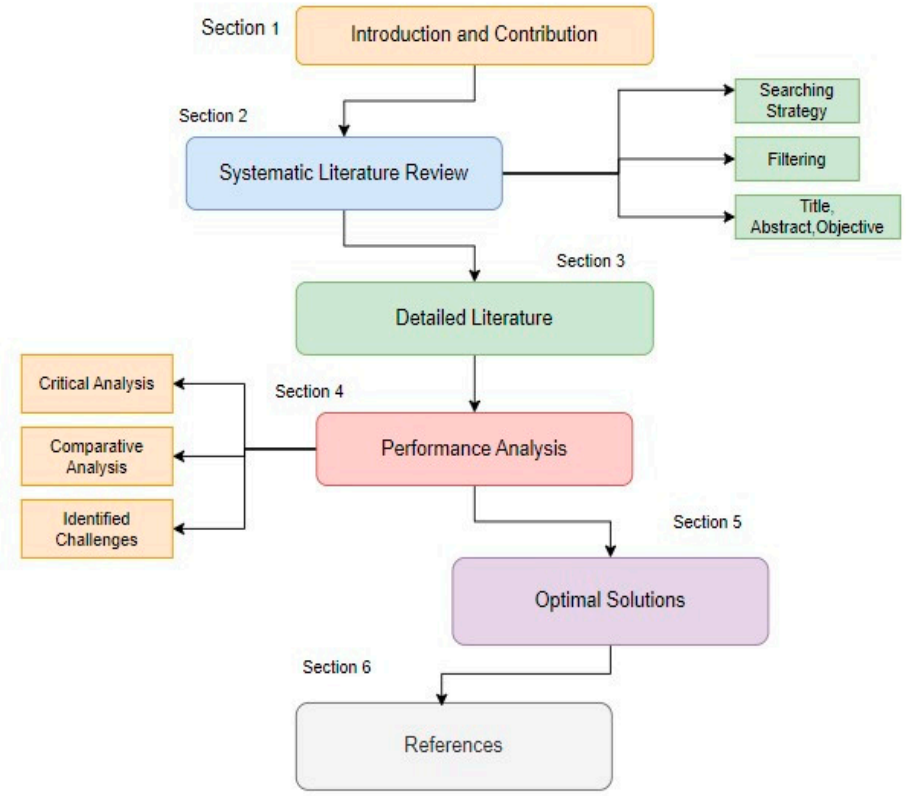

Figure 2. Paper Organization.

`This article is organized as follows: The systematic literature review procedure is covered in Section 2, the comprehensive literature review is offered in Section 3, and the performance analysis is covered in Section 4. based on examination of comparison and critical analysis. After Section 5 examines the best possibilities, Section 6 provides findings.

The paper [1] might consider a small selection of intrusion scenarios or attacks, which might not accurately represent all possible threats that a WSN might encounter. It might not make comparisons between the proposed IDS and currently deployed IDS s in the field or in literature. This can make it more difficult to evaluate the uniqueness or efficiency of the suggested IDS. Due to the low processing and memory capabilities of sensor nodes, DSs could not be scalable, especially in big WSNs. This may make it more difficult to identify and take action in response to security concerns in real-time, especially in large-scale WSNs. The Entropy weight fuzzy comprehensive evaluation approach described in [2] calls for weights to be established for each criterion. The Entropy weight fuzzy comprehensive evaluation method can only be used to evaluate quantitative data because choosing the right weights can be difficult and require subjective judgement. Its inability to evaluate qualitative data reduces its usefulness for several decision-making procedures. According to [3], the cost of implementing RFID technology on a wide scale can be high. This price may include the necessary hardware, software, as well as continuous support and maintenance, which may make it challenging for some businesses to implement the technology. The hardware, software, and communication protocols that make up the various parts of the intelligent logistics supply chain management system might not work together properly. Reduced efficiency, system problems, and communication breakdowns might follow from this. The research of [4] describes the design and validation of a traceability system based on Internet of Things (IoT) services and radio frequency identification (RFID) technology, designed to overcome the connectivity and cost-implementation issues typical in traceability systems. To track and trace the conditions of food while it is being transported, the RFID

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1641.v1

layer incorporates temperature sensors inside RFID tags. The IoT paradigm solves interconnection issues between various technology providers by allowing diverse systems to be connected to the same platform. In their study, [5], they propose a logistics tracking information management system based on a wireless sensor network that uses wireless sensor nodes to track and manage logistics tracking information. They also designed a networked logistics tracking information management system to achieve remote real-time management of logistics tracking information. It may bring up the real-time and accuracy of logistics tracking information management, which is very important for the logistics sector's information security.

2. Systematic Literature Review

The research literature discussed in this study is methodically reviewed. The systematic searches were first carried out in accordance with a search procedure that was created. These searchers were directed by the creation of strings in accordance with the determined study query. Following that, a search method was developed to classify all of the searches in accordance with the search journals. Research publications were also screened based on their title, abstract, and goals in addition to being included based on their inclusion criteria.

2.1. String Development

Three synonyms for each term were used to create the strings.

Research Question: Secure logistics monitoring system based on wireless sensor network? There will be twelve strings developed according to research question using various synonyms of each keyword.

Table 2. Ontology Table.

WORDS	SYNONYM 1	SYNONYM 2	SYNONYM 3
Secure	Protected	Riskless	Encapsulated
Logistics	Supply chain	Transportation	Management
Monitoring	Observed	Track	Check

Table 2.1. STRING DEVELOPMENT.

Secure	Protected	Riskless	Encapsulated
Secure logistics monitoring system based on wireless sensor network.			
Protected logistics monitoring system based on wireless sensor network.			
Encapsulated logistics monitoring system based on wireless sensor network.			
Riskless logistics monitoring system based on wireless sensor network.			
Secure Supply chain monitoring system based on wireless sensor network.			
Secure transportation monitoring system based on wireless sensor network			
Secure management monitoring system based on wireless sensor network.			

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1641.v1

Protected transportation system based on wireless sensor network.
Protected management system based on wireless sensor network.
Protected supply chain system based on wireless sensor network.
Encapsulated management consisting the track using wireless sensor network.
Encapsulated transportation system observed using wireless sensor network.

2.2. Searching Protocol:

In accordance with a searching procedure, articles published throughout a four-year period (2020, 2021, 2022, and 2023) were chosen for searching. Additionally, three databases (IEEE, Google Scholar, and Science Direct) and three synonyms for each keyword are included. The search techniques are displayed in Figure 3. The study topic was used to produce the strings, and publications were chosen from several databases. Of the 64 papers chosen, 15 were from IEEE, 19 were from Science Direct, and 64 were taken from the Google Scholar database.

Figure 3. Search Strategy using various Database.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1641.v1

2.3. Inclusion Criteria

According to a developed inclusion criterion, all journal articles were included. White papers were not available. Not mentioned are the articles that have not yet been published.

2.4. Filtering

In the filtering step, we first do title base filtering, followed by abstract base filtering, and finally objective base filtering on all articles that were chosen from various databases.

Figure 4 illustrates the first stage of the filtering process, which was title-based filtering. All articles from all the selected databases that we were chosen were omitted during the title base filtering since they were not pertinent to the problem's theme. Figure 4 depicts the filtering based on titles. It is evident how many studies were taken into account that are pertinent to our quest.

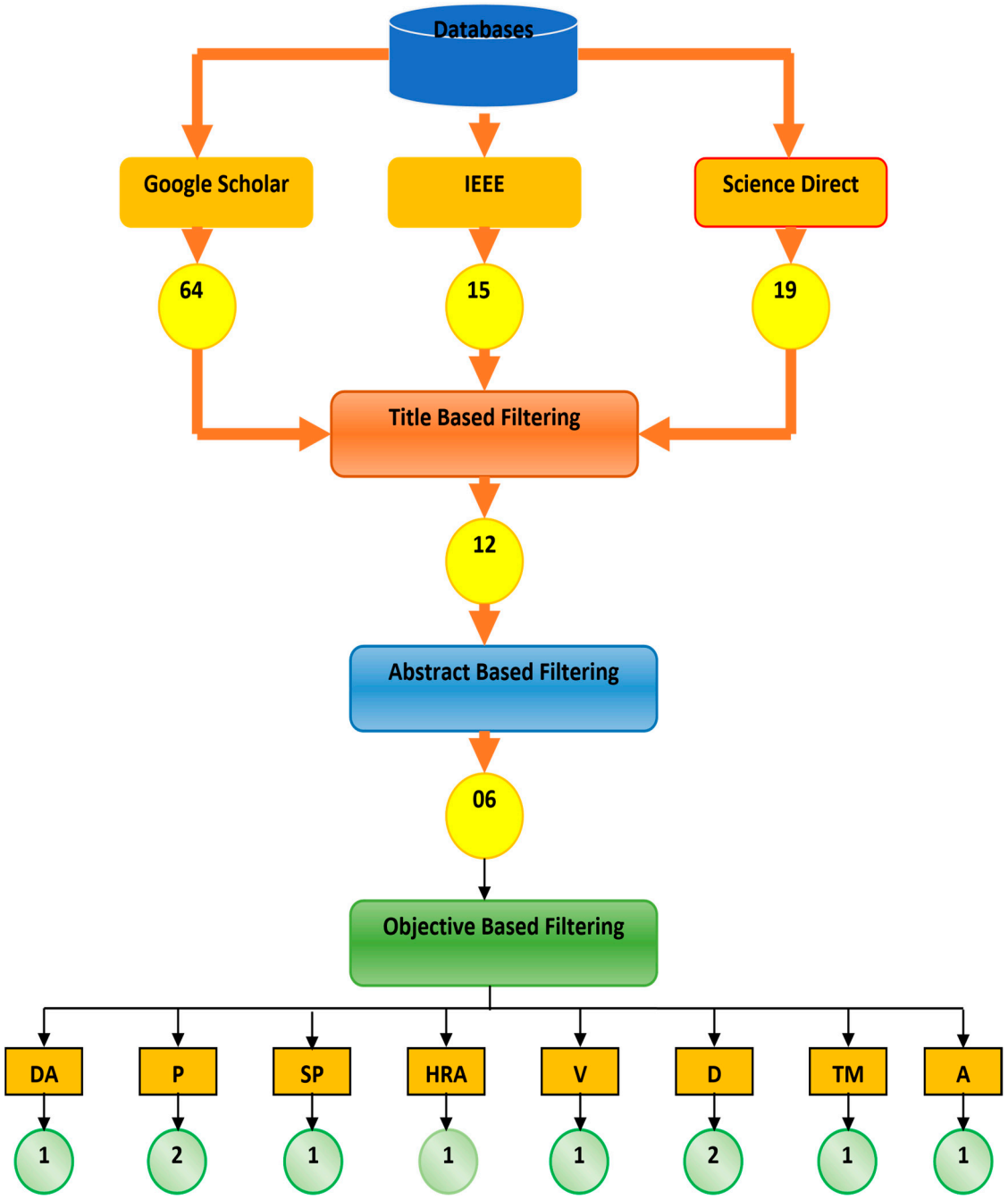

Figure 4. Screening for research articles selection to deduce the research objectives.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1641.v1

Abstract-based filtering was done in the second section. As shown in Figure 4, all publications whose abstracts were unrelated to the issue were eliminated from the databases that were chosen. All the chosen databases had all the work removed that had nothing to do with the issue.

Figure 4 illustrates the third stage of the filtering, which involved the use of objective based filtering. All materials that aren't relevant to their goals are filtered out. The sequential processes for finishing each phase are shown in Figure 4. After completing an abstract-based screening, which followed a title-based filtering, paper 06 was selected. The most current objective-based filtering chose 0 publications as having goals that matched the research topic.

A table was created showing the papers organized by their aims after all of the papers were filtered according to their objectives. The goal basis filtering, abstract base filtering, and title base filtering are displayed in Figure 4.

A table was created showing the papers organized by their aims after all of the papers were filtered according to their objectives. The acronyms used in this essay and their meanings are shown in Table 3.

Table 3. Notations and their definitions.

Acronyms	Definition
DA	Detecting Attack
P	Performance
SP	Storage positioning
HRA	High recognition accuracy
V	Validation
D	Design
TM	Time management
A	Accuracy
IDS	Intrusion Detection System
EWFEM	Entropy weight fuzzy evaluation method
RFID	Radio frequency identification

The goals of the research articles were determined and grouped into groups following the title and abstract-based grouping. This objective-based screening of the research articles under consideration is shown in Table 3, along with their relative importance for achieving those aims. The following are the categories of goals: Attack detection (DA), Performance (P), Storage positioning (SP), High recognition accuracy (HRA), Validation (V), Design (D), Time management (TM), and Accuracy (A) are the acronyms used to describe these processes.

Table 4. Objective-based screening.

Ref.	DA	P	SP	HRA	V	D	TM	A
[1]								
[2]								

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1641.v1

[3]								
[4]								
[5]								
[6]								

In the study [5], we give a taxonomy of security threats, a variety of IDS techniques for detecting assaults, and performance criteria for evaluating the IDS algorithm for WSNs. Secure communication between the sensor nodes and the base station is necessary for all WSN applications. Various threats are introduced into WSN because of adversary breaches at the sensor nodes. To protect against the security threat, a proper Intrusion Detection System (IDS) is therefore necessary in WSN. IDS strategies for WSN are categorized according to the method used to identify attacks.

A test program was created to mimic several user's login into the system simultaneously to complete tasks to assess the system's performance based on the research of [6] monitor.

The management system is tested based on the results of the research of [7] the information management process of traditional logistics company, including access, storage positioning and monitoring, and distribution monitoring and management. The results of the testing demonstrate that this system has some deployment reference relevance and practical application value, and to a certain extent, it may aid in raising the level of logistics supply chain management intelligence and achieving the study's anticipated purpose.

The research of [8] shows the design and validation of a traceability system based on Internet of Things (IoT) services and radio frequency identification (RFID) technology, designed to overcome the connectivity and cost-implementation issues prevalent in traceability systems. In order to detect and trace the conditions of food while it is being transported, the RFID layer incorporates temperature sensors inside RFID tags. The IoT paradigm solves connectivity issues between various technology providers by allowing diverse systems to be connected to the same platform.

In their research, [9] proposes a wireless sensor network-based logistics tracking information management system that uses wireless sensor nodes to track and manage logistics tracking information. They also design a networked logistics tracking information management system that allows for remote real-time management of logistics tracking information. It may bring up the real-time and accuracy of logistics tracking information management, which is very important for the logistics sector's information security.

A supply chain financial logistics oversight system is built using the Internet of Things according to [10] study. It explains the theory behind supply chain finance, smart environments, and Internet of Things technology, and it does a specific examination of the logistics supervisory system. In our exploration of a secure logistics monitoring system based on a wireless sensor network, our research draws upon foundational insights presented in [26–35]

3. Detailed Literature

Techniques:

The following table lists the methods and various procedures used in research articles.

 doi:10.20944/preprints202312.1641.v1

Table 5. Summary of methodologies of Secure logistics monitoring system.

Ref.	Technique	Methodology
[5]	Intrusion Detection System (IDS)	IDS strategies for WSN are categorized according to the method used to identify attacks. the classification of security threats, several IDS detection methods, and performance criteria for evaluating the IDS algorithm for WSNs.
[6]	Entropy weight fuzzy comprehensive evaluation method	To evaluate the platform planning scheme, use a fuzzy, comprehensive evaluation approach with entropy weight. The wireless network uses a multizone network networking technique to segment the overall coverage area into several smaller regions. Control of a sub-area is the responsibility of each wireless access point. Each wireless access point will also transform into a mobile terminal and the backbone of the network at the same time.
[7]	RFID technology	Wireless sensor network software and hardware are the foundation upon which WSN and RFID are constructed, and it is here that the intricate design of the logistics supply chain management system business process is mostly completed. The information management process of conventional logistics company, including access, storage positioning and monitoring, and distribution monitoring and management, is realized when the two primary approaches suggested in this article are combined. The management system is tested on this basis.
[8]	Radio frequency identification (RFID) technology and Service (DaaS) billing scheme	To detect and trace the conditions of food while it is being transported, the RFID layer incorporates temperature sensors inside RFID tags. The cost implementation difficulties are handled using the Data as a Service (DaaS) pricing model, which avoids the significant initial investment that these high-tech solutions frequently need by charging customers only for the data they use, rather than for the installed equipment.
[9]	JAVA technology	For design and development, the JAVA technology platform is chosen, the SQL Server database is chosen for the system's backend, and a straightforward and user-friendly WEB interface is built for the system's user service side to satisfy the demands of a userfriendly environment. The system's implementation also contributes in certain theoretical and practical ways to the design and advancement of related

 doi:10.20944/preprints202312.1641.v1

		logistics tracking information management systems based on wireless sensor networks.
[10]	Wolf group algorithm	We gather and compute logistics data using the wolf group algorithm's hunting and siege formula, and then we examine how well the logistics supervision system really performs in practice.

4. Performance Analysis

4.1. Critical Analysis

The critical evaluation of each method for identifying and preventing wormhole attacks is summarized in Table 4. There is a list of all the schemes' goals as well as their restrictions.

A WSN may not be exposed to the entire range of possible assaults that a WSN would encounter in the real world since [5] only takes a small number of intrusion scenarios or attacks into account. It might not make comparisons between the proposed IDS and already-used IDSs in the literature or in actual installations. The evaluation of the originality or efficacy of the suggested IDS may be hampered as a result. Due to the sensor nodes' constrained processing and memory capabilities, DSs could not be scalable, especially in big WSNs. Particularly with large-scale WSNs, this may make it more difficult to identify and address security concerns in real time.

The Entropy weight fuzzy comprehensive assessment approach described in [6] calls for weights to be established for each criterion. The Entropy weight fuzzy comprehensive evaluation technique can only be used to evaluate quantitative data since choosing the right weights can be difficult and involve subjective judgement. Its inability to evaluate qualitative data reduces its usefulness for several decisionmaking procedures.

In [7] RFID systems may be expensive, especially when used on a wide scale. This price may include the necessary hardware, software, as well as continuous support and maintenance, which may make it challenging for certain businesses to implement the technology. The hardware, software, and communication protocols that make up the various parts of the intelligent logistics supply chain management system could not work together properly. Reduced efficiency, system problems, and communication breakdowns could follow from this.

In [8] RFID systems may be expensive, especially when used on a wide scale. Some businesses may find it challenging to embrace the technology because of these expenses, which may not be fully disclosed up front by DaaS providers. These costs may include hardware, software, and ongoing maintenance and support. For instance, there can be extra charges for bandwidth consumption or data storage that are not accounted for in the initial cost. Some DaaS vendors have inflexible price structures that prevent modification. For clients with certain usage patterns or requirements, this may be an issue.

In [9] Compared to programs written in other languages like C or C++, Java programs often run more slowly. This is due to the performance impact of Java programmers' need to be interpreted or compiled at runtime. Java applications have a tendency to use a lot of memory, which can be problematic for applications that must operate on systems with memory constraints.

The use of IoT technology in supply chain management raises privacy and security problems, which [10] may not sufficiently address. This can hinder the system's acceptance and usefulness in practical situations. It might not offer a thorough cost benefit analysis of the suggested solution, which might restrict its usefulness in actual situations.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1641.v1

Table 6. Summary of critical analysis of logistics monitoring system.

Detection Algorithm	Effort Year	Technique	Short coming
[5]	2020	Intrusion Detection System (IDS)	Inability to respond or stop attacks upon detection [11] Scalability issue [12]
[6]	**2021**	Entropy weight fuzzy comprehensive evaluation method	Difficulty in determining weights and limited to quantitative data [13] Security Vulnerabilities [14]
[7]	2023	RFID technology	Not as accurate, reliable expensive or Compatibility issues [15] Cost and Scalability [16]
[8]	**2023**	Radio frequency identification (RFID) technology and Service (DaaS) billing scheme	RFID is less precise and reliable. Expensive. The cost of the service (DaaS) pricing model is greater, and there is less customization and control [17]. To prevent unauthorized access and data breaches in such systems, security and privacy safeguards must be developed [18].
[9]	2023	JAVA technology	It is very slow and has restrictions on platforms [19] The algorithm may still spend a lot of energy if it is not energy-efficient, which might shorten the life of WSN nodes and decrease the efficiency of the system [20].
[10]	**2021**	Wolf group algorithm	Lack of privacy and security. Cost-effectiveness [21] To defend the system from cyber-attacks, it is crucial to establish strong security measures including encryption, access control, and data backup. [22]

Research Gap:

The following Table shows the gaps in previous studies and their solution are also discussed below.

Table 7. Research Gap.

Ref.	Research Gaps	Solutions
[5]	Low Scalability issue	Hierarchical IDS architecture that uses a clustering algorithm
[13]	Difficult weight determination	Load cell sensor and a calibration method
[14]	High Security Vulnerabilities	Advanced Encryption Standard (AES) to secure
[20]	Low optimization and reduced effectiveness	Integration with other systems
[21]	Issue of security and privacy	Wolf group algorithm

Conclusion

This study identified the security and privacy challenges in smart logistics systems, the source of cyber-attacks prevalent in smart logistics contracts, which is a critical issue for the optimal operation of logistics operations. This research paper made a valuable contribution to mitigating security and privacy concerns in intelligent logistics systems by introducing a logistics management system that utilizes Cryptographic Hash Functions. By implementing Role-Based Access Control, this system bolsters security against cyber-attacks and ensures the privacy of customer data when shared among various logistics stakeholders. The results indicate that the utilization of Cryptographic Hash Functions for sharing customer data among logistics partners effectively protects against cyber-attacks. The proposed system ensures asset security, and based on the case study evaluation, demonstrates resilience against a wide range of security and privacy threats. Despite its importance, this study has certain limitations. One of the limitations is the substantial overlap between research on logistics and supply chain management (SCM). While our focus primarily centered on logistics tasks, the broader context of SCM was not extensively explored.

References

1. Elsisi, M.; Mahmoud, K.; Lehtonen, M.; Darwish, M.M.F. Reliable Industry 4.0 Based on Machine Learning and IoT for Analyzing, Monitoring, and Securing Smart Meters. Sensors 2021, 21, 487.
2. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. Comput. Netw. 2010, 54, 2787–2805.
3. WSN based Online Parameter Monitoring in Cold Storage Warehouses in Cloud using IOT concepts Bindu J, Nikitha, Namitha, Pradeep H, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 07 | July-2018 www.irjet.net p-ISSN: 2395-0072.
4. J. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial Internet: A survey on the enabling technologies, applications, and challenges," IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1504–1526, 3rd Quart., 2017.
5. S. Godala, R. Prasad, and V. Vaddella, "An Intrusion Detection System in Wireless Sensor Networks," *Int. J. Commun. Netw. Inf. Secur. IJCNIS*, vol. 12, pp. 127–141, Apr. 2020, doi: 10.17762/ijcnis.v12i1.4429.
6. "Intelligent Logistics Tracking System Based on Wireless Sensor Network," *Int. J. Front. Eng. Technol.*, vol. 3, no. 10, 2021, doi: 10.25236/IJFET.2021.031006.

7. "Optimization of Intelligent Logistics Supply Chain Management System Based on Wireless Sensor Network and RFID Technology." https://www.hindawi.com/journals/js/2021/8111909/ (accessed Feb. 28, 2023).
8. "Sensors | Free Full-Text | Cost-Effective Implementation of a Temperature Traceability System Based on Smart RFID Tags and IoT Services." https://www.mdpi.com/14248220/20/4/1163 (accessed Feb. 28, 2023).
9. "Using Wireless Sensor Network to Remote Real-Time Monitoring and Tracking of Logistics Status Based on Difference Transmission Algorithm." https://www.hindawi.com/journals/js/2021/4084288/ (accessed Feb. 28, 2023).
10. "Construction of a Supply Chain Financial Logistics Supervision System Based on Internet of Things Technology." https://www.hindawi.com/journals/mpe/2021/9980397/ (accessed Mar. 04, 2023).
11. Wang, C., Li, J., & Zhang, H. (2018). An Intrusion Detection System in Wireless Sensor Networks. Journal of Physics: Conference Series, 1101, 012027.
12. Kshetri, N., Voas, J., & An, Y. (2019). Intrusion detection in wireless sensor networks: A comprehensive review. Journal of Network and Computer Applications, 125, 60-78. doi: 10.1016/j.jnca.2018.11.017
13. Jing, Z., Li, J., Li, J., & Li, X. (2016). Design and Implementation of Intelligent Logistics Tracking System Based on Wireless Sensor Network. 2016 IEEE 2nd International Conference on Big Data Analysis (ICBDA), 16-19.
14. Zhang, X., Wang, K., Xiang, T., & Zhao, M. (2020). A survey on wireless sensor network-based intelligent logistics tracking systems. Journal of Network and Computer Applications, 168, 102711. doi: 10.1016/j.jnca.2020.102711
15. Tang, J., Yan, X., & Feng, Q. (2014). Research on the Interoperability of RFID Technology in Supply Chain Management. In Proceedings of the International Conference on Logistics, Informatics and Service Sciences (LISS) (pp. 25-28). IEEE.
16. Shi, Y., Yuan, Q., Cao, H., & Cui, L. (2021). Optimization of logistics supply chain management system based on wireless sensor network and RFID technology: A review. Journal of Ambient Intelligence and Humanized Computing, 12(3), 2843-2863. doi: 10.1007/s12652-020-02647-7
17. Kumar, A., & Garg, S. (2020). A cost-effective implementation of temperature traceability system based on smart RFID tags and IoT services. Journal of Food Science and Technology, 57(2), 467-475. doi: 10.1007/s13197-019-04096-2
18. Xu, S., Cheng, S., & Zhou, Y. (2021). Security and privacy challenges in RFID and IoT-based temperature monitoring systems. Sensors, 21(3), 745. doi: 10.3390/s21030745
19. Xu, Q., Qiu, Y., Yan, L., & Lu, H. (2017). Design of wireless sensor network for remote real-time monitoring and tracking of logistics status based on difference transmission algorithm. International Journal of Distributed Sensor Networks, 13(8), 1550147717723741. doi: 10.1177/1550147717723741
20. Huang, Y., Yu, H., & Wu, J. (2020). An energy-efficient differential data transmission scheme for wireless sensor networks. Sensors, 20(13), 3739. doi: 10.3390/s20133739
21. Zhang, Z., Wang, J., Zhang, S., & Song, H. (2020). Construction of a supply chain financial logistics supervision system based on internet of things technology. International Journal of Distributed Sensor Networks, 16(4), 1550147720913349. doi: 10.1177/1550147720913349
22. Kamble, S. S., Saini, S., & Patel, R. (2021). A review on IoT-based supply chain management system: Challenges, applications, and future scope. Journal of Industrial Integration and Management, 6(1), 21-40. doi: 10.1080/21681015.2020.1840649
23. Amin R, Islam S K H, Biswas G P, et al. Design of an anonymity-preserving threefactor authenticated key exchange protocol for wireless sensor networks[J]. Computer Networks, 2016, 101(6):42-62.
24. Ding X, Tian Y, Yu Y, A Real-Time Big Data Gathering Algorithm Based on Indoor Wireless Sensor Networks for Risk Analysis of Industrial Operations[J]. IEEE Transactions on Industrial Informatics, 2016, 12(3):1232-1242.
25. Hussain, K., Hussain, S. J., Jhanjhi, N. Z., & Humayun, M. (2019, April). SYN flood attack detection based on bayes estimator (SFADBE) for MANET. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-4). IEEE.
26. Adeyemo Victor Elijah, Azween Abdullah, NZ JhanJhi, Mahadevan Supramaniam and Balogun Abdullateef O, "Ensemble and Deep-Learning Methods for Two-Class and Multi-Attack Anomaly Intrusion Detection: An Empirical Study" International Journal of Advanced Computer Science and Applications(IJACSA), 10(9), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100969
27. Lim, M., Abdullah, A., & Jhanjhi, N. Z. (2021). Performance optimization of criminal network hidden link prediction model with deep reinforcement learning. Journal of King Saud University-Computer and Information Sciences, 33(10), 1202-1210.
28. Kumar, T., Pandey, B., Mussavi, S. H. A., & Zaman, N. (2015). CTHS based energy efficient thermal aware image ALU design on FPGA. *Wireless Personal Communications*, *85*, 671-696.

29. Diwaker, C., Tomar, P., Solanki, A., Nayyar, A., Jhanjhi, N. Z., Abdullah, A., & Supramaniam, M. (2019). A new model for predicting component-based software reliability using soft computing. IEEE Access, 7, 147191-147203.
30. Hussain, S. J., Ahmed, U., Liaquat, H., Mir, S., Jhanjhi, N. Z., & Humayun, M. (2019, April). IMIAD: intelligent malware identification for android platform. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.
31. Humayun, M., Alsaqer, M. S., & Jhanjhi, N. (2022). Energy optimization for smart cities using iot. Applied Artificial Intelligence, 36(1), 2037255.
32. Ghosh, G., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). Secure surveillance system using chaotic image encryption technique. In IOP conference series: materials science and engineering (Vol. 993, No. 1, p. 012062). IOP Publishing.
33. Almusaylim, Z. A., Zaman, N., & Jung, L. T. (2018, August). Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment. In 2018 4th International conference on computer and information sciences (ICCOINS) (pp. 1-5). IEEE.
34. Wassan, S., Chen, X., Shen, T., Waqar, M., & Jhanjhi, N. Z. (2021). Amazon product sentiment analysis using machine learning techniques. Revista Argentina de Clínica Psicológica, 30(1), 695.
35. Shahid, H., Ashraf, H., Javed, H., Humayun, M., Jhanjhi, N. Z., & AlZain, M. A. (2021). Energy optimised security against wormhole attack in iot-based wireless sensor networks. Comput. Mater. Contin, 68(2), 1967-81.