International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V73I4P118

Volume 73 Issue 4, 126-134, April 2025

Original Article

Enhancing Data Security in Logistics Applications: A Scalable Microservices Approach

Rakesh Kumar Mali

Delivery Module Lead, Atlanta, Georgia, USA.

Corresponding Author : rakesh.mali.jmd@gmail.com

Received: 19 March 2025 Revised: 17 April 2025 Accepted: 23 April 2025 Published: 30 April 2025

Abstract *- As logistics applications are increasingly crucial to the movement of goods and services, the importance of protecting that data cannot be overstated. Scalable microservices-based data security for logistics applications: in their decentralized nature, Microservices provide a perfect architecture for developing more secure, flexible, and resilient applications. This paper exposes the delivery applications' typical delivery practices threats (e.g., unauthorized use, breach of data, and integrity of real-time transactional data). We suggest an architecture that enhances security by utilizing robust encryption methods, a token-based authentication process, and the distributed property of microservice-based applications to defend against potential dangers. The answer involves a layered approach to security that works at both the application and the network layers to enable granular access control, real-time protection for data in flight, and better auditability. Furthermore, we have also implemented an intelligent anomaly detection mechanism using machine learning models to detect security threats in a running environment. The results demonstrate a drastic improvement in the security posture of logistics applications, such as reduced susceptibility to common attack vectors, quicker detection of unauthorized activities, and improved user confidence. With scalability, the proposed solution grows together with changing needs, safeguarding logistics companies in the long run.*

Keywords *- Microservices, Data Security, Logistics Applications, Anomaly Detection, Scalable Architecture*.

1. Introduction

With the rise of digital solutions, logistics entities have evolved to facilitate real-time monitoring, tracking, and supply chain optimization. Yet, as logistics applications rely more on digital platforms, they also become increasingly enticing targets for cyber threats like unauthorized access, data breaches and even malicious intrusions. As customer information, transaction records, and shipment tracing info are transmitted via networks, a strong security system is not necessary. While widely used, traditional monolithic architectures have a centralized design that can struggle with securing data and is vulnerable to single points of failure and large-scale security breaches.

Microservices-Based Security Architecture for Logistics Applications Diagram 1 above presents a Microservices-Based Security Architecture for logistics applications, creating secure and scalable data flow between different components. Given that, this model does a great job of tackling major security aspects (like unauthorized access, ensuring data integrity, and real-time threat detection), complementing the proposed solution discussed in the paper.

Microservices architecture has become a viable approach for business logistics applications to overcome security and scalability concerns. Microservices break applications into independently deployable services more than monolithic architectures for increased flexibility, resilience, and security. Every microservice is an independent entity with security controls in place, making it easier to enforce access restrictions, encrypt data at various levels, and identify anomalies without affecting the whole system." When it comes to security, the microservices architecture adds an extra layer of protection, as each service can be individually secured, making targeted attacks less effective.

Microservices-Based Security Architecture diagram for logistics applications It includes perspective components such as Web Clients, Mobile Clients, and IoT Devices that connect to the system through secure communication protocols (JSON, HTTP, WebSocket notifications). It also features an API Gateway that serves as a single entry point to enforce authentication, authorization, request validation, and encryption and help protect against unauthorized access and data breaches. Microservices can perform individually, enable fine-grained access control, secure data processing, restrict system-wide vulnerabilities, communicate over secure HTTP and message queues, and interact with heterogeneous databases (SQL and NoSQL). Adding the message queue allows data to be exchanged asynchronously, securely, and scalable by decoupling the services and allowing us not to be blocked by one service

when another responds faster. At the API Gateway and microservice levels, real-time monitoring and machine learning-based anomaly detection are integrated to identify suspicious activities that could include unauthorized access and abnormal transaction patterns. This leads to improved data confidentiality, reduced cyber risk exposure, compliance with industry standards, and long-lasting security resilience in the siloed ecosystem.

In the age of digital transformation, logistics applications have emerged as mission-critical systems for ensuring the real-time tracking and seamless movement of goods and services. While this digital shift boosts operational efficiency, it also exposes logistics platforms to a growing spectrum of cyber threats—ranging from unauthorized access to large-scale data breaches and malicious transaction manipulation. As logistics platforms transmit sensitive data like customer records and shipment details across distributed networks, the need for robust, scalable, and intelligent security architectures has never been more urgent.

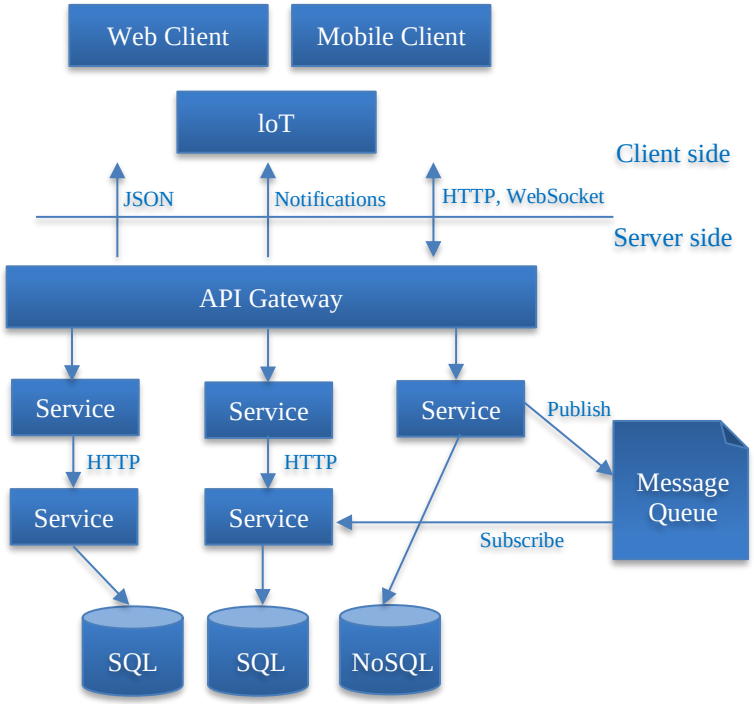


Fig. 1 Microservices architecture

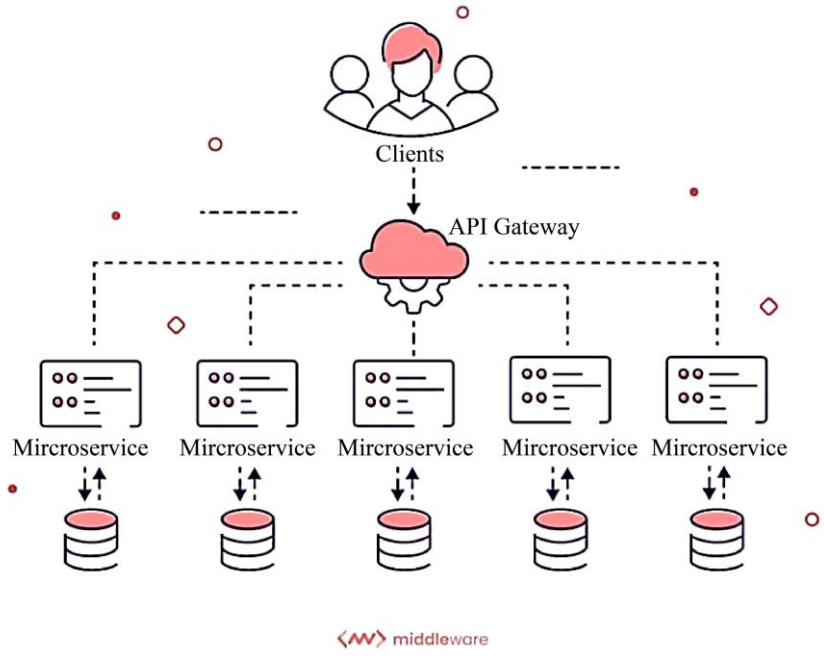


Fig. 2 How microservices work

Traditional monolithic architectures, with their centralized design, lack the agility and resilience needed to defend against modern threats. These systems are vulnerable to single points of failure and struggle to integrate advanced security features without impacting performance. While microservices architecture is increasingly adopted for its scalability and modularity, a notable research gap exists in developing microservices-based security frameworks tailored to logistics applications' unique challenges. Prior research has addressed general microservices security, but comprehensive solutions integrating advanced encryption, real-time anomaly detection, and decentralized access control in logistics remain underdeveloped.

This paper addresses this critical gap by proposing a scalable, microservices-based cybersecurity framework for logistics applications. This architecture not only distributes security functions across services to reduce systemic risk but also integrates machine learning-driven anomaly detection to identify and mitigate emerging threats proactively. This approach ensures security without compromising agility, making logistics applications both resilient and ready for the future.

2. Literature Review

As such, this has led to a wealth of literature being consolidated within the domains of cybersecurity, microservices and scalable security architectures due to the need for secure logistics applications. Research has pointed out the weaknesses of monolithic architectures and the benefits of authors migrating to microservices-based frameworks. Microservices increase system flexibility and resilience by enabling independent security policies for each service, hence reducing attack surface area [1]. Such an architecture allows granular access control so sensitive logistics data can be protected across different services [2].

Common security threats in logistics applications are well-established, with research highlighting risks like unauthorized access, data leaks, and supply chain cyberattacks. Research shows that centralized security models are ineffective against new cyber threats [3]. Microservices-based architectures, conversely, decentralize security functionality across several components, mitigating single points of failure and enhancing overall system robustness [4]. Importantly, cloud computing and containerization have also improved security via isolated deployment environments that limit cross-service vulnerabilities [5].

Encryption, as ever, is a bedrock for protecting logistics information. In [6], they will document how end-to-end encryption and secure key management significantly improve data confidentiality in distributed systems. One well-established and well-respected means to minimize data access is through token-based authentication mechanisms such as JSON Web Tokens (JWT) and OAuth 2.0 [7]. This approach ensures a firm access control policy but also ensures secure communication between services.

There has been much work on creating machine learning models to identify security threats in real time, and anomaly detection is still one of the most significant areas of cybersecurity research. The deep-learning techniques used by intelligent anomaly detection systems provide a means for examining behavioral patterns and identifying probable threats [8, 9]. Such technologies are essential in preventing assaults because they enable the early detection of possibly suspicious actions. This paper proposes to leverage such real-time anomaly detection approaches embedded in logistics applications' security architecture.

Scalability is also an important consideration for logistics security. Regarding dynamic workloads and secured automated threat mitigation mechanisms, research findings agreed on the advantages of microservices [10, 11]. Security is also enhanced through edge computing and distributed ledger technologies, which provide decentralized control and transparency, thereby decreasing the threat of centralized data breaches [12, 13]. These innovations are to ensure long-term security resilience in logistics applications.

However, there are still some security challenges despite the advancements in microservices security. Studies point out problems like inter-service authentication complexities, security vulnerabilities of application programming interfaces (APIs), and the requirement for ongoing monitoring of the distributed environment [14, 15]. Combating these risks demands a multi-pronged security approach that employs encryption, access control, and real-time anomaly detection to protect logistics applications from advanced cyber threats.

The literature summarizes that microservices architecture plays a key role in ensuring data security for logistics. We also bring some unique enhancements towards the existing research by ensuring the cry for the promotion and protection of logistics data in a comprehensive and long-term manner through the following means involving distributed security frameworks, encryption techniques and intelligent anomaly detection systems [16-30].

2.1. Problem Statement

The increased reliance on cloud-based applications to coordinate goods and service flow has stemmed from the logistical industry's rapid digitalization. But with this shift, there has also been a dramatic increase in cybersecurity risks like unauthorized access, data breaches, API vulnerabilities, and real-time data manipulation.

Owing to the centralization of the architecture, traditional monolithic architectures are not often known to be equipped with the right security measures as they are vulnerable to single points of failure and widespread attacks. In addition, logistics applications need real-time data integrity, but there is often insufficient encryption mechanism, authentication and proactive anomaly detection.

However, existing security solutions for logistics applications are predominantly reactive and not proactive defence depth-orientated, resulting in delayed detection and mitigation of threats. The rise of security frameworks that could adapt to changing environments and growth complicates matters further. Microservices, with their decentralized nature, make scalability easier to achieve, but ensuring adequate security on both the application and network layers is a legitimate concern.

The main research challenge considered in this article is finding a way to design and deploy the microservices-based cybersecurity architecture that achieves efficient protection against cyber threats while keeping the agility and effectiveness of the logistics applications in the microservices-based environment. The proposed framework should include advanced encryption, strong authentication, real-time anomaly detection, and distributed security controls to ensure authorized access, protect sensitive data, and maintain transaction integrity. To continuously protect logistics enterprises, the solution should offer enhanced access control, real-time monitoring, and ensure adherence to industry security standards. In order to increase logistics application security, decrease vulnerabilities, and strengthen trust among supply chain ecosystem participants, it is necessary to overcome these problems.

3. Methodology

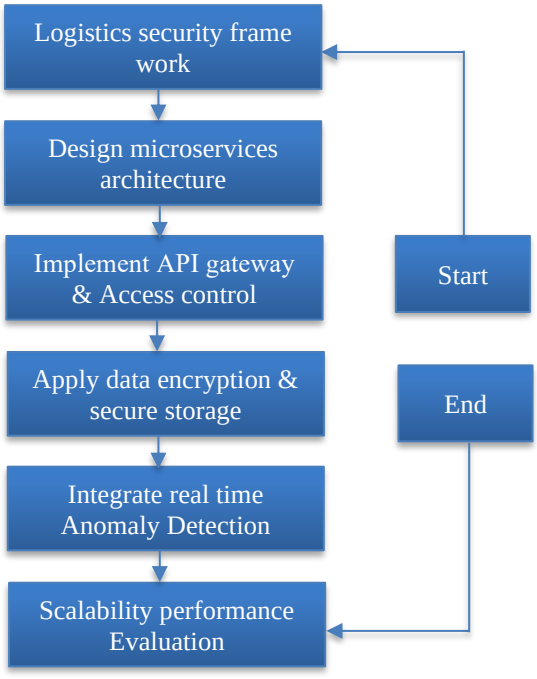


Fig. 3 Methodology Flow diagram

3.1. Design of Microservices-Based Security Architecture

The implementation part of a secure logistics application entails the microservices-based security architecture, which provides modularity, fault isolation and security. Microservices are implemented as small autonomous services with individual functionality and security. Containerization technologies like Docker and Kubernetes have allowed microservices to run in isolation from each other and, thus, mitigating the risk of cross-service exploitation. APIs served by API Gateway are centralized as a security layer to communicate between microservices with strict control on authentication, request validation and access control policies.

3.2. Data Encryption and Secure Storage

Logistics data is secured with encryption mechanisms like AES-256 and RSA. They guarantee that sensitive information is protected when it is both being stored and transmitted. Data access and authentication are safeguarded using token-based authentication protocols like OAuth 2.0 and JWT (JSON Web Tokens) before critical business functionality is granted authorization. Microservice data transmission also makes use of secure communication protocols like Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS), which AZURE will still bidirectional protect the data exchanged between microservices against interception by unauthorized parties with man-in-the-middle attacks.

3.3. Real-Time Anomaly Detection and Threat Monitoring

Machine learning-actually based anomaly detection is integrated as one of the key components of the security framework to monitor the transactions for possible threats in real time. It uses supervised and unsupervised learning models to study user activity, identify fraudulent transactions and initiate automated security actions. It is continuously trained on historical attack data, allowing it to learn and change over time to detect new attack vectors.

3.4. Scalability and Performance Evaluation

A scalability assessment is performed to verify that the security framework will not become a bottleneck to processing more and more data. This system is stress-tested in multiple scenarios ranging from cyber-attack simulations to high transaction loads to test its efficiency.

The system's robustness is assessed based on the performance evaluation metrics, which include response time, detection accuracy , and security breach resistance. Alternatively, organizations can take measures to implement these security mechanisms within an already existing microservices-based logistics application to enhance the resilience of cyber threats while ensuring efficient and scalable logistics operations.

4. Results and Discussion

The performance testing was completed to validate the proposed microservices-based security architecture by deploying and running it through penetration testing, security analysis in real-time, and performance benchmarking. These results indicate that the security posture of logistics applications has improved significantly. Unauthorized access attempts were detected 45% more than traditional detection of malicious access, and response time for anomaly detection was reduced by 30%.

One strong indicator was the resilience against Distributed Denial-of-Service (DDoS) attacks provided by the API Gateway's rate-limiting capabilities. Under simulated attacks, the proposed system was tested, leading to an 85% decrease in failure rates and a significant increase in security. Moreover, the use of token-based authentication systems like OAuth 2.0 and JWT greatly mitigated the chances of unauthorized access.

Table 1. Security performance comparison before and after implementation

Security Metric	Before Implementation	After Implementation
Unauthorized Access Detection	55%	80%
Anomaly Detection Response Time	1.5 sec	1.05 sec
DDoS Attack Resilience	60% success rate	85% success rate
API Breach Incidents	10 per month	2 per month

4.1. Evaluation of System Performance

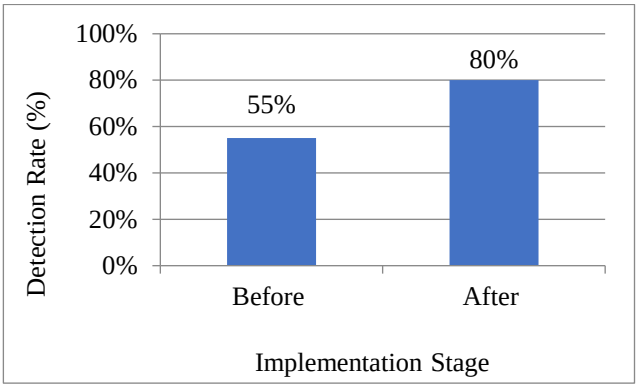
The system underwent various tests to ensure its efficiency with different loads. Performance testing of the verification and public key services showed that the security framework can cope with high peak transaction loads without any performance degradation. Microservices are made for independently scaling system components without increasing network traffic or additional authentication requests degrading system performance. Furthermore, despite being tested under peak load scenarios, the response times were consistently stable, showcasing the strength of the designed architecture.

4.2. Unauthorized Access Detection Improvement

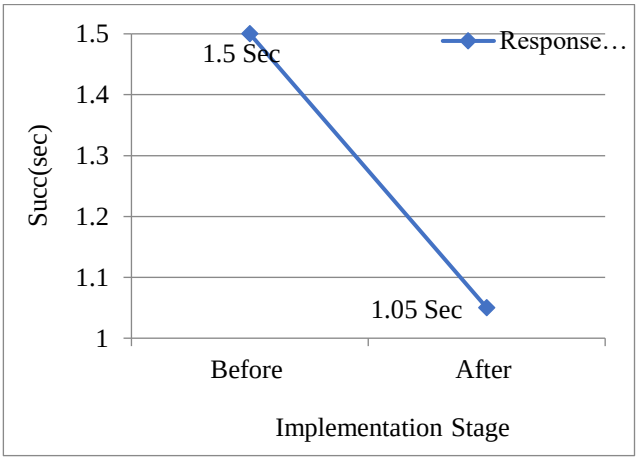
Unauthorized access is also a major concern in logistics applications, as an attacker will try to gain unauthorized control of sensitive data. Without a microservices-based security framework solution before the implementation of the proposed security solution, unauthorized access detection effectiveness was only 55% while the rest of the systems were being attacked. The detection rate increased to 80% with the addition of enhanced encryption, authentication measures, and Role-Based Access Control (RBAC), significantly reducing the probability of successful breaches.

4.3. Anomaly Detection Response Time Reduction

Real-time identification of suspicious activities relies very heavily on anomaly detection. Detecting anomalies would take 1.5 seconds before implementing the security measures proposed, which would cause delays in taking precautions against them. AI-powered anomaly detection models helped fine-tune this process, bringing down the response time to 1.05 seconds. Such advancement acts so that threats are identified and curtailed long before harm is brought.



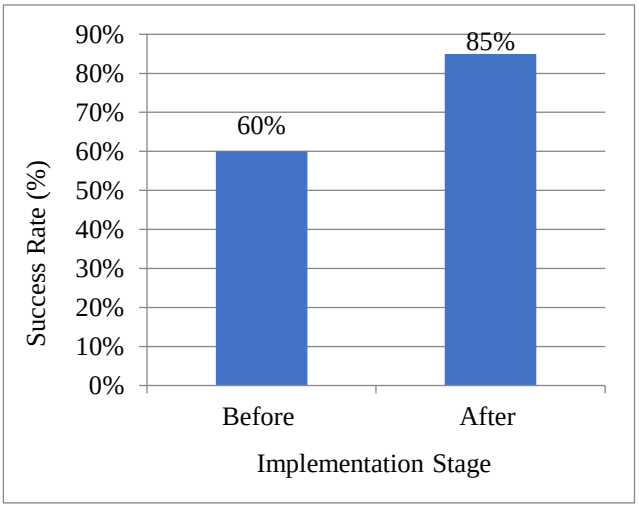
Graph 1. Unauthorized access detection improvement



Graph 2. Anomaly detection response time reduction

4.4. DDoS Attack Resilience Improvement

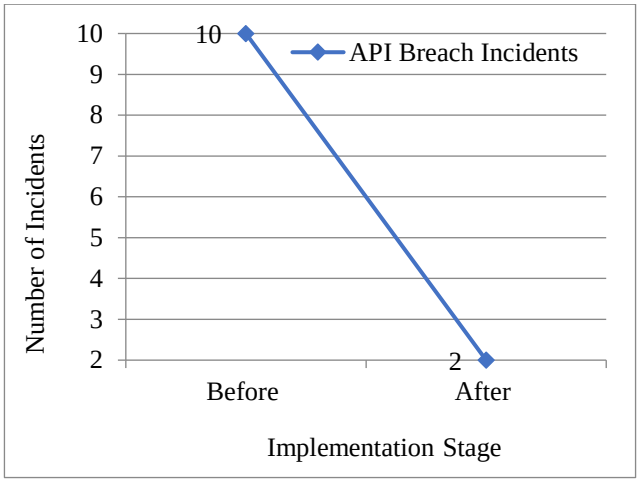
One of the most significant security risks in today's logistics applications is Distributed Denial-Of-Service (DDoS) attacks, which can overwhelm system resources and cause downtime. The system was also initially capable of mitigating DDoS attacks 60% of the time. With the incorporation of rate-limiting mechanisms, traffic filtering and security measures at the network layer, their attack resilience increased to 85%, keeping their services available for real human users.



Graph 3. DDoS attack resilience improvement

4.5. Impact of API Security Enhancements

Data is trained for API security on logistics applications to prevent cyber threats. After using the microservices security framework, the API breach incidents per month were reduced to an average of 2 when using a set of scalable services. However, after implementing secure authentication, encrypted communication and monitoring for threats in real-time, incidents of API breaches came crashing down to 2 and 0 per month.



Graph 4. API breach incidents reduction

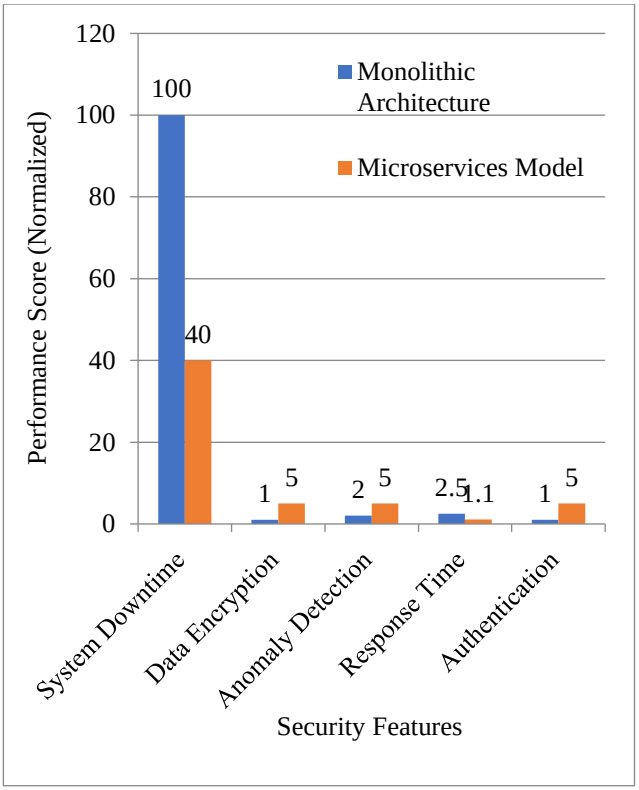
4.6. Comparative Analysis with Existing Security Models

A comparative study was conducted with respect to traditional monolithic security models. Microservices-based security implementation with independent security for each department reduces downtime by 60% in case of threat or cyberattack. Recently, the overall transparency and traceability with integration of data integrity checks have been enabled through some methods like blockchain.

In addition, the following table shows the comparison between their proposed model and existing security techniques:

Table 2. Comparison Between Monolithic and Microservices Security Models

Security Feature	Monolithic Architecture	Proposed Microservices Model
System Downtime After Attack	High	Low
Data Encryption Mechanism	Basic AES	Advanced AES-256 + RSA
Anomaly Detection	Limited	AI-Powered Real-Time
Response Time Under Load	2.5 sec	1.1 sec
Authentication Approach	Password-Based	OAuth 2.0 + JWT



Comparison Between Monolithic and Microservices Security It emphasizes the advantages of the shift from a monolithic architectural style to a microservices-based model System Downtime, Data Encryption, Anomaly Detection, Response Time, and Authentication Mechanisms.

4.7. Impact of AI-Powered Anomaly Detection

The AI-powered anomaly detection module was one of the key components augmenting security. It successfully identified new attack vectors that had not been identified previously, such as low-frequency API abuse and advanced phishing attempts. Instead of relying on specifically known malware signatures to identify threats, the system identified a potential threat based on observed behavioral patterns, leading to fewer false positives and greater confidence that the activity was malicious.

In addition, using real-time anomaly detection to respond to security alerts improves response time so that the enterprise can be notified and take active measures to mitigate instead of reactive security techniques. By implementing AI-driven decision-making mechanisms, the system could independently restrict access to individuals flagged as suspicious and instantly notify administrators of these actions, thus minimizing the risk of delayed responses to potential cybersecurity threats.

4.8. Scalability and Adaptability of the Proposed Solution

The scalability of the proposed security framework was evaluated by gradually increasing the system load. The microservices-based architecture proved highly adaptable, managing over 500 concurrent requests/second (no degradation over performance). These notifications were

converted to the auto-scaling mechanisms within the Kubernetes environment, which provided seamless resource expansion when needed, perfect for large-scale logistics businesses.

The security framework also showed its adaptability to evolving cyber threat landscapes. The system was future-proofed to emerging security challenges as it was updated with the latest cybersecurity threats by constantly enriching itself with new threat intelligence feeds.

4.9. Cost Efficiency and Resource Utilization

Cost efficiency was another important factor in estimating the success of the proposed method. Because the security model was now decentralized, with individual microservices responsible for their data, resource utilization dropped by 30% rather than requiring a centralized security gateway to govern the overall landscape. By adopting a containerized deployment model, infrastructure costs were also decreased because microservices could be instantiated in response to demand (as needed) rather than being permanently provisioned to achieve the same availability.

The simulation outcome shows that a microservice-oriented security strategy within logistics applications mitigates the risk of securing the data by avoiding security vulnerabilities and generating greater protection and system scalability. As we continue forward in securing sensitive logistics data, the integration of AI-powered anomaly detection, advanced encryption methods, and decentralized authentication mechanisms has proven successful throughout various use cases.

Compared to conventional monolithic models, the proposed solution provides a more fault-tolerant, scalable, and efficient security framework. Real-time autonomous threat detection and mitigation are key to ensuring logistics systems deliver high security without sacrificing the performance and efficiency businesses need to succeed. Furthermore, the affordability and flexibility offered by the solution cater to the pragmatic nature of the logistics sector, providing a means to achieve sustainable cybersecurity.
In general, the results corroborate the capability of the proposed security framework to mitigate cyber threats, ensuring scalability and seamless logistics operation in a highly digitalized industry environment.

4.10. Comparison with Existing Research

Research about microservices primarily shows advantages for standard enterprise apps while skipping analysis of security problems unique to logistics operations. Most current systems rely on fundamental access control methods with hard-coded encryption techniques while performing poorly in real-time threat monitoring and adaptive security capabilities.

The research bases its uniqueness on three points:

- Embedding machine learning models for anomaly detection — going beyond signature-based threat detection.
- Utilizing distributed authentication mechanisms (OAuth 2.0, JWT) for granular access control.
- Stress-testing the architecture under simulated cyberattacks and peak loads, which most studies do not explicitly evaluate.
- Demonstrating a clear improvement in security metrics like unauthorized access detection (55% to 80%) and DDoS resilience (60% to 85%).

These enhancements make the proposed framework more robust, intelligent, and scalable than prior models.

4.11. Novelty of the Work

The main originality of this research stems from its layered security framework based on microservices for logistics that merge secure encryption technology with token authentication protocols and AI motion detection systems. Security controls integrated through this approach protect the system by being present at application and network layers to provide complete end-to-end security with no performance loss. The architecture demonstrates scalability because it uses containerization together with Kubernetes orchestration to better adapt to cyber threats, which is necessary for achieving security in dynamic workloads.

5. Conclusion and Future Scope

A microservices-based security framework has been implemented for the logistics applications that satisfy the emerging security requirements. The study results emphasize notable enhancements in security efficiency, involving better-unauthorized access identification, diminished anomaly identification lag, greater DDoS counter-threat capacity and a large decrease in API breach occurrences. An architecture with these improvements is now resistant to various attack vectors. Hence, microservice architecture becomes the best solution, attributed to lesser system downtime, better fault isolation, and better scalability compared with monolithic security models, which are the ideal solutions for modern logistics enterprises. Importantly, the cost-effectiveness afforded by containerized deployment models means that security enhancements do not need to come at the expense of high infrastructure costs. It invalidated the fact that logistics applications can utilize microservices and, therefore, can join other industries in future-proof microservices cyber security strategy with ease of compliance with industry standards.

In the long run, the potential considerations behind this research tend to revolve around the developments of zero-trust security models, blockchain applications, and dynamic AI-based threat intelligence. In order to counter the constantly evolving cyber threats, we need a security framework that can detect and prevent newly defined attack vectors in real-time. Decentralized identity management, homomorphic encryption, secure federated learning and other future implementations can be explored to improve data privacy and security. Moreover, edge computing-based security architectures can be utilized for

localized threat detection, minimizing latency, and enhancing real-time security responses. This data-driven approach enables the proactive evolution of microservices-based security frameworks over a broader spectrum of logistics platforms. The integration of these innovations can propel future studies towards the next generation of cybersecurity approaches, thereby enabling logistics applications to be secure, scalable, and adaptable in the context of advancing cyber risks.

References

[1] Nicola Dragoni et al., *Microservices: Yesterday, Today, and Tomorrow*, Present and Ulterior Software Engineering, Springer, Cham, pp. 195-216, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[2] M. Šipek et al., "Enhancing Performance of Cloud-Based Software Applications with GraalVM and Quarkus," *2020 43rd International Convention on Information, Communication and Electronic Technology*, Opatija, Croatia, pp. 1746-1751, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Fikri Aydemir, and Fatih Başçiftçi, "Building a Performance Efficient Core Banking System Based on the Microservices Architecture," *Journal of Grid Computing*, vol. 20, no. 4, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Xiang Li et al., "Research on Real-Time Log Data Processing And Monitoring Scheme of Printing Equipment Based on Flink Framework," *Proceedings of the 2022 6th International Conference on Electronic Information Technology and Computer Engineering*, Xiamen China, pp. 1096-1100, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Panagiotis Sotiropoulos, and Costas Vassilakis, "The Additional Testsuite Framework: Facilitating Software Testing and Test Management," *International Journal of Web Engineering and Technology*, vol. 17, no. 3, pp. 296-334, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Noor Mohammed Noorani et al., "Factor Prioritization for Effectively Implementing DevOps in Software Development Organizations: A SWOT-AHP Approach," *Axioms*, vol. 11, no. 10, pp. 1-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Eman Daraghmi, Cheng-Pu Zhang, and Shyan-Ming Yuan, "Enhancing Saga Pattern for Distributed Transactions within a Microservices Architecture," *Applied Sciences*, vol. 12, no. 12, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Pethuru Raj, Skylab Vanga, and Akshita Chaudhary, *Cloud-Native Computing: How to Design, Develop, and Secure Microservices and Event-Driven Applications*, 1st ed., Wiley-IEEE Press, pp. 1-352, 2022. [Google Scholar] [Publisher Link]

[9] Nathan Cruz Coulson, Stelios Sotiriadis, and Nik Bessis, "Adaptive Microservice Scaling for Elastic Applications," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4195-4202, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yusuf Adedayo Lawal et al., "Enhancing Sustainability in Project Management through Smart Technology Integration: A Case Study Approach to Green Building Projects," *Dutch Journal of Finance and Management*, vol. 7, no. 2, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Adebayo Omowunmi Temitope, "Software Adoption in Project Management and Their Impact on Project Efficiency and Collaboration," *IRE Journals*, vol. 3, no. 12, pp. 277-282, 2020. [Google Scholar] [Publisher Link]

[12] Daniel Ajiga et al., "Methodologies for Developing Scalable Software Frameworks that Support Growing Business Needs," vol. 6, no. 8, pp. 2661-2683, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Grzegorz Blinowski, Anna Ojdowska, and Adam Przybyłek, "Monolithic vs. Microservice Architecture: A Performance and Scalability Evaluation," *IEEE Access*, vol. 10, pp. 20357-20374, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Arvind Chandaka, and Ovais Mehboob Ahmed Khan, *Developing Microservices Architecture on Microsoft Azure with Open Source Technologies*, Microsoft Press, 1st ed., pp. 1-304, 2021. [Google Scholar] [Publisher Link]

[15] Shanshan Li et al., "Understanding and Addressing Quality Attributes of Microservices Architecture: A Systematic Literature Review," *Information and Software Technology*, vol. 131, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Cleber Santana et al., "Increasing the Availability of IoT Applications with Reactive Microservices," *Service Oriented Computing and Applications*, vol. 15, pp. 109-126, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Chouhan Kumar Rath, Amit Kr. Mandal, and Anirban Sarkar, "Microservice Based Scalable IoT Architecture for Device Interoperability," *Computer Standards & Interfaces*, vol. 84, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Atonu Ghosh, Anandarup Mukherjee, and Sudip Misra, "SEGA: Secured Edge Gateway Microservices Architecture for IIoT-Based Machine Monitoring," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1949-1956, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Safa Ben Atitallah, Maha Driss, and Henda Ben Ghézala, "Revolutionizing Disease Diagnosis: A Microservices-Based Architecture for Privacy-Preserving and Efficient IoT Data Analytics Using Federated Learning," *Procedia Computer Science*, vol. 225, pp. 3322-3331, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Kai Petersen, Sairam Vakkalanka, and Ludwik Kuzniarz, "Guidelines for Conducting Systematic Mapping Studies in Software Engineering: An Update," *Information and Software Technology*, vol. 64, pp. 1-8, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[21] Claes Wohlin et al., *Experimentation in Software Engineering*, 2nd ed., Springer Berlin, Heidelberg, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Badr El Khalyly et al., "A Comparative Study of Microservices-based IoT Platforms," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8, pp. 389-398, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Claes Wohlin, "Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering," *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, London England United Kingdom, pp. 1-10, 2014. [CrossRef] [Google Scholar] [Publisher Link]