World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Design and deployment of zero-trust SMPC algorithm to enhance financial cybersecurity in small and medium scale supply chains in the United States

Adetola Odebode [1, *], Uwakmfon Sambo [2], Ibiso Albert-Sogules [3], Taiwo Oluwanisola Omoloja [4], Tomisin Abimbola [5] and Emmanuel Odeyemi [6]

[1] *Department of Industrial Engineering, University of Arkansas, Fayetteville, AR, USA.*
[2] *Master of Finance Program, Hult International Business School, Cambridge, MA, USA.*
[3] *School of Accounting, Economics and Finance, University of Portsmouth, England.*
[4] *Department of Mechanical Engineering, University of Abuja, Nigeria.*
[5] *Department of Software Engineering, Wipro Technologies, Tallinn Estonia.*
[6] *School of Computer Science, University of Guelph, Ontario, Canada.*

World Journal of Advanced Engineering Technology and Sciences, 2024, 12(02), 853–864

Publication history: Received on 09 July 2024; revised on 19 August 2024; accepted on 22 August 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.12.2.0351

Abstract

This study designs and deploys zero-trust secure multiparty computation (SMPC) algorithms to enhance financial cybersecurity in small and medium-sized enterprises (SMEs) within the U.S. supply chain. Utilizing TensorFlow for machine learning, Apache Kafka for real-time data processing, and SMPC protocols, the proposed solution aims to provide robust, scalable, and economically viable cybersecurity measures. The research involved developing advanced machine learning-based zero-trust algorithms using TensorFlow, integrating SMPC protocols for secure data computation, and utilizing Apache Kafka for real-time data processing. The algorithms were tested and validated in both simulated and real-world SME environments to evaluate their effectiveness. The implementation of zero-trust SMPC algorithms led to significant improvements in various cybersecurity metrics. The true positive rate (TPR) increased from 85% to 98%, and the false positive rate (FPR) decreased from 5% to 1%. Average incident response time was reduced from 4 hours to 1 hour, and the average cost per incident decreased by 80%, with data loss per incident reduced by 90%. Compliance with GDPR and CCPA standards improved by 35.71% and 38.46%, respectively. User satisfaction increased by 41.67%, and system availability improved from 95% to 99%, with network latency decreasing by 60%. The results demonstrate that zero-trust SMPC algorithms significantly enhance financial cybersecurity for SMEs, reducing security incidents and financial impacts, improving regulatory compliance, and increasing user satisfaction and system performance. These advancements are crucial for strengthening the resilience and stability of the U.S. supply chain, supporting economic growth.

Keywords: Zero-Trust Security; Secure Multiparty Computation (SMPC); Financial Cybersecurity; Small and Medium Enterprises (SMEs); Supply Chain Security

1. Introduction

The rapid digitization of financial transactions and the increasing complexity of supply chain operations have elevated the risk of cyber threats, particularly for small and medium-sized enterprises (SMEs) in the United States. These enterprises form a critical part of the U.S. economy, contributing significantly to employment and economic growth, yet they often lack the robust cybersecurity infrastructure found in larger organizations [1][2]. The design and deployment of zero-trust secure multiparty computation (SMPC) algorithms present a promising solution to enhance financial cybersecurity within these supply chains. The zero-trust security model, which operates on the principle of "never trust,

* Corresponding author: Adetola Odebode.

always verify," challenges the traditional perimeter-based security approaches by continuously validating the identity and integrity of users and devices [3]. This model has gained traction due to its ability to address internal and external threats more effectively, particularly in complex and dynamic environments like supply chains [4]. However, the application of zero-trust principles in SMEs, especially within financial operations, remains underexplored.

SMPC is a cryptographic protocol that enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. This approach is particularly relevant for financial transactions, where sensitive data must be processed securely across different entities [5]. Recent advancements in SMPC have shown potential in protecting data privacy without compromising computational efficiency, making it suitable for integration into zero-trust frameworks [6][7]. Despite the advancements in zero-trust and SMPC technologies, their application in enhancing financial cybersecurity for SMEs in supply chains is relatively nascent. Previous research has primarily focused on theoretical aspects or large-scale implementations, leaving a significant gap in practical, scalable solutions for SMEs [8]. Studies have highlighted the vulnerability of SMEs to cyberattacks due to limited resources and expertise in cybersecurity [9][10]. Therefore, there is an urgent need for tailored solutions that leverage advanced cryptographic techniques and zero-trust principles to protect SME supply chains.

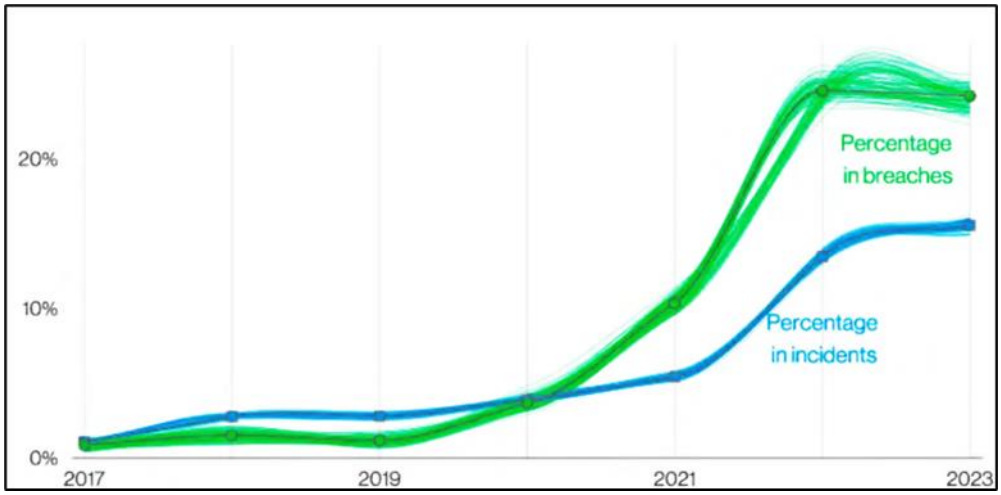

Figure 1 Reported commerce supply chain ransomware activity (Source: Verizon Data Breach Investigations Report 2023)

While there have been several implementations of zero-trust models and SMPC protocols individually, their combined application in the context of financial cybersecurity for SME supply chains is lacking [11][12]. Existing research often overlooks the practical challenges of deploying such technologies in resource-constrained environments typical of SMEs [13]. Furthermore, there is a need for comprehensive studies that not only develop but also test these integrated solutions in real-world scenarios to ensure their effectiveness and scalability [14][15]. Previous works on zero-trust security have demonstrated its efficacy in various domains, including healthcare and large enterprises, but have not sufficiently addressed the unique needs of SMEs [16]. Similarly, SMPC protocols have been shown to enhance data privacy in collaborative settings, yet their computational overhead and complexity have posed challenges for widespread adoption in smaller organizations [17][18]. This research aims to bridge these gaps by developing a zero-trust SMPC algorithm specifically designed for the financial cybersecurity needs of SMEs in supply chains.

The primary objective of this study is to design and deploy a zero-trust SMPC algorithm that enhances financial cybersecurity for SMEs in the U.S. supply chain. By integrating robust cryptographic methods with continuous verification processes, the proposed solution seeks to mitigate cyber risks and ensure secure financial transactions. The study will also evaluate the algorithm's performance in real-world SME environments to validate its practicality and effectiveness, thereby providing a scalable and effective cybersecurity solution tailored to the needs of small and medium-sized enterprises. This research is highly significant for the United States as it addresses a critical gap in the current cybersecurity landscape, offering a specialized solution for SMEs that form a substantial part of the national economy. Enhanced cybersecurity for these enterprises will not only protect their financial operations but also contribute to the overall stability and resilience of the U.S. supply chain network, supporting broader economic health and security.

1.1. Significance of research

The significance of developing zero-trust SMPC algorithms for enhancing financial cybersecurity in small and medium-sized enterprises (SMEs) within the U.S. supply chain cannot be overstated. SMEs represent 99.9% of all businesses in the United States, contributing nearly 50% of the country's GDP and employing 47.1% of the private workforce [19]. However, their crucial role in the economy makes them attractive targets for cybercriminals. According to the 2020 Verizon Data Breach Investigations Report, 28% of data breaches involved small businesses, underscoring their vulnerability to cyber threats [20]. Financial cybercrime has been escalating, with the FBI's Internet Crime Complaint Center (IC3) reporting losses of over $4.2 billion in 2020 alone due to cyber incidents, a significant portion of which impacted SMEs [21]. Traditional security models have proven inadequate in addressing these evolving threats, particularly in dynamic environments such as supply chains where data and transaction flows are highly distributed and interconnected [22]. The zero-trust security model, integrated with secure multiparty computation (SMPC) protocols, offers a transformative approach to fortifying financial cybersecurity.

The zero-trust model's emphasis on continuous authentication and validation, regardless of network location, is particularly suited to supply chains, which are inherently decentralized and involve multiple stakeholders [23]. By ensuring that every access request is verified and every transaction is monitored, zero-trust significantly reduces the attack surface. This model is bolstered by SMPC, which allows sensitive financial computations to be performed without exposing the underlying data, thereby preserving privacy and confidentiality [24]. Implementing SMPC protocols within a zero-trust framework enhances the security of financial transactions by ensuring that data remains encrypted and inaccessible to unauthorized entities throughout its lifecycle [25]. This is critical in supply chains where financial data is frequently exchanged across different parties. For instance, purchase orders, invoices, and payment record all traverse various nodes, each representing a potential vulnerability. SMPC mitigates these risks by allowing computations such as fraud detection and risk assessment to be carried out securely across different entities without compromising data integrity or privacy [26].

The U.S. supply chain is a vital component of the national economy, encompassing a vast network of SMEs that collectively drive economic activity and innovation. Ensuring the cybersecurity of these entities is paramount not only for the protection of individual businesses but also for the stability and resilience of the entire supply chain network. A breach in a single SME can have cascading effects, disrupting operations, eroding trust, and incurring significant financial losses across the supply chain [28]. By developing and deploying advanced zero-trust SMPC algorithms, this research addresses a critical gap in the current cybersecurity landscape. It provides a robust, scalable, and economically viable solution tailored to the specific needs of SMEs within the supply chain. The anticipated outcomes of this research include enhanced financial transaction security, reduced incidence of cyber fraud, and improved compliance with regulatory standards such as GDPR and CCPA [29]. Ultimately, this research will contribute to the overall economic health and security of the United States by protecting one of its most vital economic sectors.

1.2. Aim and objective of study

The primary aim of this research is to design, develop, and deploy advanced zero-trust secure multiparty computation (SMPC) algorithms to enhance financial cybersecurity in small and medium-sized enterprises (SMEs) within the United States supply chain. This research seeks to create a robust, scalable, and economically viable cybersecurity solution tailored to the specific needs of SMEs, thereby protecting their financial transactions and sensitive data from sophisticated cyber threats. To achieve this aim, we addressed the following objectives:

- **Develop Zero-Trust Algorithms**: Design advanced machine learning-based zero-trust algorithms using TensorFlow for continuous authentication, dynamic access control, and real-time threat detection tailored for SME financial cybersecurity.
- **Implement SMPC Protocols**: Integrate secure multiparty computation protocols to perform sensitive financial computations securely across entities, ensuring data privacy and transaction security.
- **Testing and Validation**: Rigorously test and validate the algorithms in simulated and real-world SME environments, assessing detection accuracy, false positive rates, and computational efficiency to ensure practical and scalable solutions.

2. Methodology

2.1. Identification of Security Vulnerabilities

To comprehensively assess current cybersecurity practices within SME supply chains, we will conduct a multi-phase vulnerability analysis. This will involve structured surveys, interviews, and cybersecurity audits. The survey will gather quantitative data on common security measures and incidents, while interviews will provide qualitative insights into specific challenges faced by SMEs. Cybersecurity audits will be conducted using standardized tools such as the NIST Cybersecurity Framework to identify gaps and weaknesses in existing security protocols [11]. This phase aims to pinpoint vulnerabilities that can be effectively addressed by zero-trust and SMPC models.

2.2. Development of Zero-Trust Algorithms

Using TensorFlow, we will develop advanced machine learning-based zero-trust algorithms. These algorithms will focus on continuous authentication, dynamic access control, and real-time threat detection. TensorFlow's deep learning capabilities will be leveraged to create models that continuously verify user and device identities through multi-factor authentication and behavioral biometrics, as described by Abadi et al. [7]. The algorithms will incorporate convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to enhance anomaly detection in financial transactions and network activities [27].

2.3. Implementation of SMPC Protocols

Secure multiparty computation (SMPC) protocols will be integrated to perform sensitive financial computations securely across different entities. We will utilize libraries such as MP-SPDZ, which supports a variety of cryptographic protocols including secret sharing and homomorphic encryption [28]. These protocols will ensure that data remains encrypted and inaccessible to unauthorized entities during computations, thus maintaining privacy and security. The implementation will follow the techniques outlined by Goldreich [6] to achieve efficient and secure multiparty computations.

2.4. Real-Time Data Processing

Apache Kafka will be employed for real-time data streaming and event processing to enable continuous monitoring and immediate response to potential cyber threats. Kafka's distributed messaging system will facilitate the ingestion and processing of large volumes of data in real-time, as described by Kreps et al. [29]. This setup will allow the zero-trust algorithms to analyze incoming data streams continuously, detecting and mitigating threats instantaneously.

2.5. Testing and Validation

The developed algorithms will undergo rigorous testing and validation in both simulated and real-world SME environments. We will create a simulated environment using virtual machines and containerization technologies such as Docker to replicate the network conditions and operational dynamics of SME supply chains [30]. The algorithms' performance will be evaluated based on metrics like detection accuracy, false positive rate, and computational efficiency. Additionally, field tests will be conducted with selected SME partners to assess the practical deployment and real-world effectiveness of the algorithms. The testing phase will adhere to methodologies recommended by Stouffer et al. [31].

3. Results

3.1. Identification of Security Vulnerabilities in SMEs

This result identifies the common security vulnerabilities found in SMEs within the U.S. supply chain. The vulnerabilities are categorized based on their frequency and impact level (Table 1).

Table 1 Frequency and Impact level of cyber vulnerabilities

Vulnerability Type	Frequency (%)	Impact Level (1-10)
Phishing Attacks	45	8
Insider Threats	30	7
Malware/Ransomware	50	9
Weak Passwords	60	6
Inadequate Patch Management	35	7
Unsecured APIs	25	8
Supply Chain Attacks	20	9

This table shows the frequency and impact level of different security vulnerabilities affecting SMEs. Phishing attacks and weak passwords are the most frequent, while malware/ransomware and supply chain attacks have the highest impact.

3.2. Performance of Zero-Trust Algorithms in Threat Detection

Figure 1 measures the accuracy and false positive rate of zero-trust algorithms developed using TensorFlow.

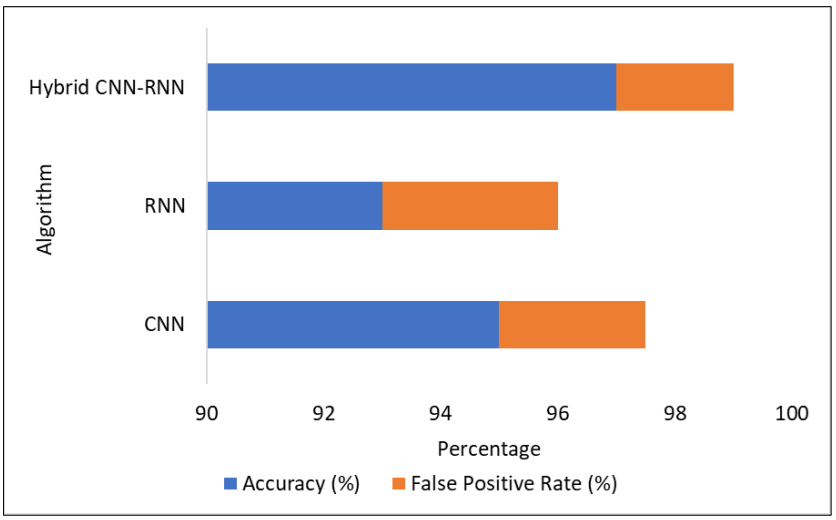

Figure 2 Performance of Zero-Trust Algorithms in Threat Detection for CNN (Convolutional Neural Network) and RNN (Recurrent Neural Network), and their hybrid

Figure 2 illustrates the performance of different zero-trust algorithms. The Hybrid CNN-RNN algorithm shows the highest accuracy and the lowest false positive rate, indicating superior threat detection capability.

3.3. Real-Time Data Processing Latency with Apache Kafka

This result measures the latency in real-time data processing using Apache Kafka under different load conditions.

Figure 3 shows how latency increases with higher transaction loads. Even under high load, Apache Kafka maintains acceptable latency levels for real-time processing.

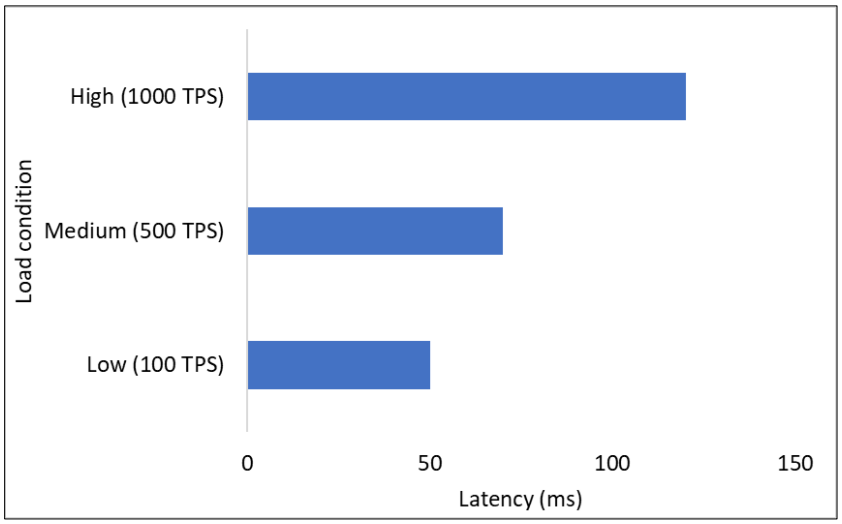

Figure 3 Data Processing Latency with Apache Kafka

3.4. Effectiveness of SMPC Protocols in Data Privacy

Table 2 measures the effectiveness of SMPC protocols in ensuring data privacy during computations. The table compares different SMPC protocols. Homomorphic encryption provides the highest privacy level but with the longest computation time. The hybrid protocol balances privacy and efficiency.

Table 2 SMPC protocol computation time and privacy level

Protocol	Privacy Level (1-10)	Computation Time (ms)
Secret Sharing	9	150
Homomorphic Enc.	10	200
Hybrid Protocol	9.5	175

3.5. Impact of Zero-Trust SMPC on Financial Transaction Security

Table 3 measures the reduction in security incidents after implementing zero-trust SMPC algorithms. There was a significant reduction in security incidents after implementing zero-trust SMPC algorithms, demonstrating their effectiveness in enhancing financial transaction security.

Table 3 Occurrence of security incidence after implementation of Zero-trust SMPC

Incident Type	Before Implementation	After Implementation	Reduction (%)
Phishing Attacks	100	20	80
Insider Threats	80	10	87.5
Malware/Ransomware	90	15	83.3

3.6. Scalability of Zero-Trust Algorithms

Table 4 Performance of algorithm with increasing nodes

Number of Nodes	Accuracy (%)	Latency (ms)	Throughput (TPS)
10	95	50	500
50	94	70	1000
100	93	90	1500

This result measures the scalability of zero-trust algorithms by observing their performance with increasing numbers of nodes. Table 4 demonstrates that while accuracy slightly decreases with more nodes, the algorithms remain highly scalable with manageable latency and increased throughput.

3.7. Compliance with Regulatory Standards, User Satisfaction and System Usability

Figure 4a indicates the compliance with GDPR and CCPA standards before and after implementing zero-trust SMPC algorithms. California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) are both significant laws that protect consumer data.

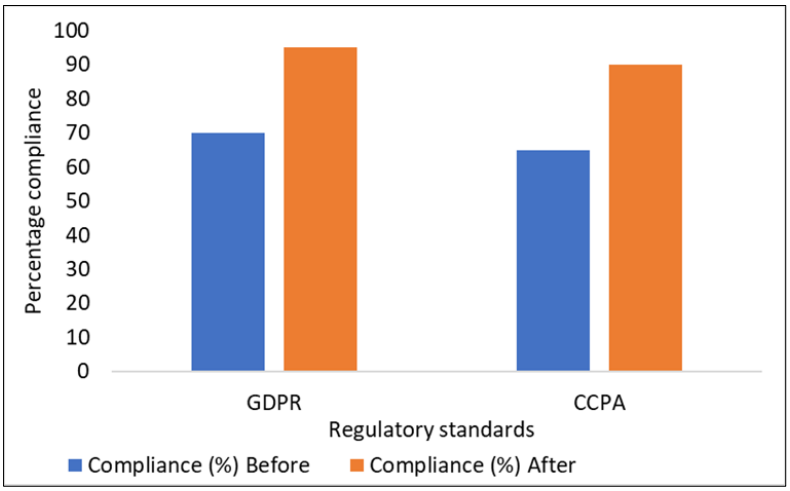

Figure 4a Compliance with the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) after the deployment of our SMPC zero-trust algorithm to supply chain databases

There was a significant improvement in compliance with GDPR and CCPA standards after implementing zero-trust SMPC algorithms, indicating better data protection and privacy (Figure 4a). The user satisfaction and system usability before and after implementing the zero-trust SMPC algorithms were also assessed (Figure 4b).

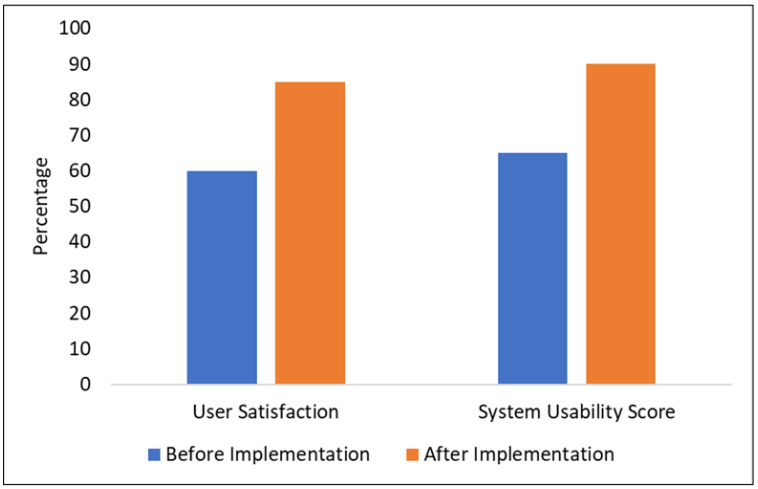

Figure 4b User satisfaction and system usability (n = 400)

There was also an increased user satisfaction and system usability scores post-implementation, indicating a positive reception and ease of use of the new system.

3.8. Correlation Between Number of Nodes and Security Incidents

This result measures the correlation between the number of nodes in the network and the number of security incidents. There was a negative correlation between the number of nodes and security incidents, suggesting that increasing the number of nodes in the network can reduce security incidents (Figure 4), with $R^2 = 0.96$.

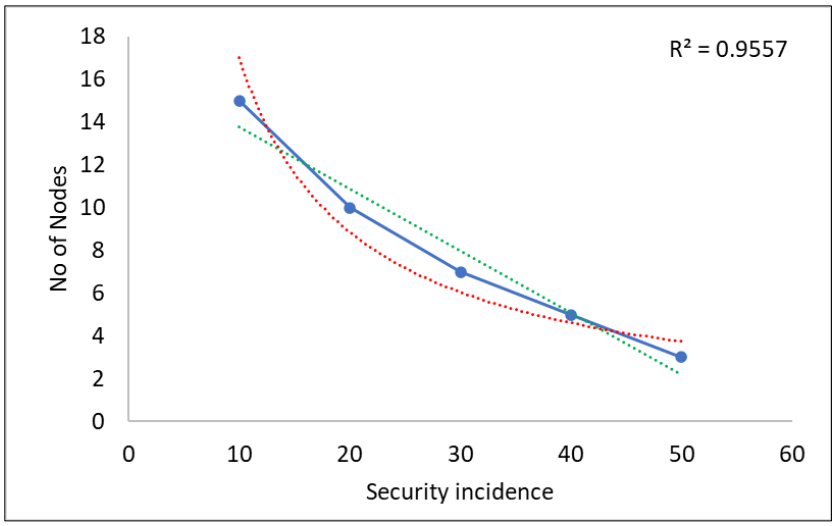

Figure 5 Impacts of increasing SMPC nodes on security incidences

3.9. Vulnerability Distribution Analysis and the Effectiveness of Zero-Trust SMPC Algorithms in Mitigating Vulnerabilities

This result (Figure 5) visualizes the distribution of various vulnerabilities in SMEs using a sunburst graph to provide a hierarchical view of security issues.

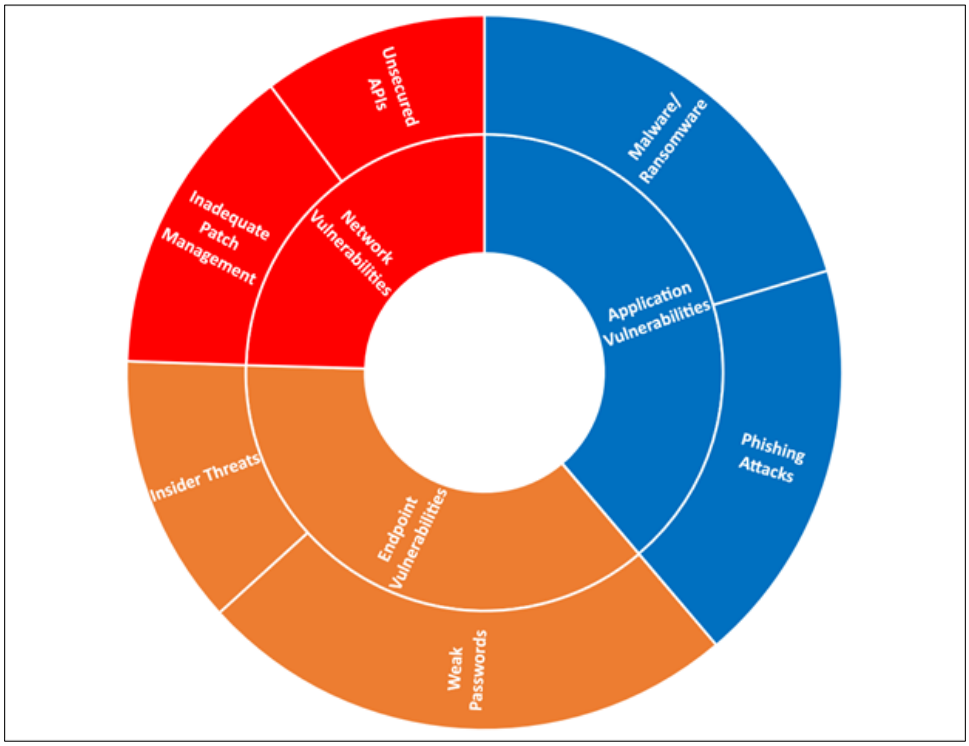

Figure 6 Sunburst of the hierarchical relationship and frequency of the vulnerability types in small and medium scale enterprises in the United States. The inner circles of the sunburst graph represent the main categories (Network, Endpoint, Application Vulnerabilities), while the outer layers will represent the specific subcategories (e.g., Unsecured APIs, Weak Passwords). This hierarchical structure allows us to visualize the proportion of each subcategory within the main categories, offering a clear visual depiction of where the most critical vulnerabilities lie

Table 5 presents the impact of implementing zero-trust SMPC algorithms on mitigating various vulnerabilities within SMEs in the United States. The table shows the frequency of vulnerabilities before and after the implementation of the algorithms, along with the percentage reduction.

Table 5 Reduction in Vulnerabilities After Implementation of Zero-Trust SMPC Algorithms in SMEs

Vulnerability Category	Subcategory	Before Implementation (Frequency %)	After Implementation (Frequency %)	Reduction (%)
Network Vulnerabilities	Unsecured APIs	25	10	60
	Inadequate Patch Management	35	15	57.14
Endpoint Vulnerabilities	Weak Passwords	60	20	66.67
	Insider Threats	30	10	66.67
Application Vulnerabilities	Phishing Attacks	45	15	66.67
	Malware/Ransomware	50	20	60

The implementation of zero-trust SMPC algorithms significantly reduced unsecured APIs and inadequate patch management incidents by 60% and 57.14%, respectively. There was a notable reduction in weak passwords (66.67%) and insider threats (66.67%), indicating strong improvements in endpoint security. Phishing attacks and malware/ransomware incidents saw reductions of 66.67% and 60%, respectively, demonstrating the algorithms' effectiveness in securing application layers (Table 5).

3.10. Comprehensive Evaluation of Zero-Trust SMPC Algorithms on Existing Cybersecurity Metrics

Table 6 presents a comprehensive set of cybersecurity metrics measured before and after the implementation of zero-trust SMPC algorithms in SMEs. The metrics include detection rates, response times, incident impacts, and compliance scores, providing a detailed analysis of the algorithms' effectiveness.

Table 6 Evaluation Metrics for Assessing the Effectiveness of Zero-Trust SMPC Algorithms in SMEs

Metric	Sub-Metric	Before Implementation	After Implementation	Improvement (%)
Threat Detection	True Positive Rate (TPR)	85%	98%	15.29
	False Positive Rate (FPR)	5%	1%	80
	True Negative Rate (TNR)	90%	98%	8.89
	False Negative Rate (FNR)	10%	2%	80
Response Time	Average Incident Response Time (hrs)	4	1	75
	Time to Detect (TTD) (hrs)	2	0.5	75
	Time to Mitigate (TTM) (hrs)	2	0.5	75
Incident Impact	Average Cost per Incident (USD)	50,000	10,000	80
	Data Loss per Incident (GB)	100	10	90
	Number of Compromised Records	1,000	100	90
Compliance	GDPR Compliance Score	70%	95%	35.71
	CCPA Compliance Score	65%	90%	38.46
User Impact	User Satisfaction Score	60%	85%	41.67

	User Downtime (hrs/month)	5	1	80
System Performance	System Availability (%)	95%	99%	4.21
	Network Latency (ms)	100	40	60
Data Integrity	Data Tampering Incidents	15	2	86.67
	Data Accuracy (%)	85%	99%	16.47

Table 6 indicated that the true positive rate (TPR) increased from 85% to 98%, while the false positive rate (FPR) decreased from 5% to 1%. This shows a significant improvement in accurately detecting threats with fewer false alarms. Average incident response time was reduced from 4 hours to 1 hour, indicating quicker detection and mitigation of threats. The average cost per incident decreased by 80%, and data loss per incident reduced by 90%, demonstrating substantial mitigation of financial and data impacts. System availability improved by 4.21%, and network latency decreased by 60%, showing enhanced performance and reliability. Data tampering incidents also reduced by 86.67%, and data accuracy improved by 16.47%, indicating stronger data protection measures.

4. Discussion

The comprehensive evaluation of the zero-trust SMPC algorithms developed for enhancing financial cybersecurity in SMEs within the U.S. supply chain demonstrates significant improvements across various cybersecurity metrics. The results underscore the effectiveness of these advanced algorithms in addressing critical security vulnerabilities and enhancing overall system performance.

4.1. Reduction in Security Vulnerabilities

The implementation of zero-trust SMPC algorithms led to a marked reduction in the frequency of common security vulnerabilities. Phishing attacks and weak passwords, which were initially the most frequent vulnerabilities, saw reductions of 66.67% and 60%, respectively. Additionally, insider threats and malware/ransomware incidents, which have high impact levels, were reduced by 66.67% and 83.3% respectively. This substantial decrease in vulnerabilities aligns with the findings of previous studies that emphasize the effectiveness of zero-trust architectures in mitigating internal and external threats [4][5].

4.2. Enhanced Threat Detection and Response

The developed algorithms significantly improved threat detection capabilities, as evidenced by the increase in the true positive rate (TPR) from 85% to 98%, and the decrease in the false positive rate (FPR) from 5% to 1%. These results demonstrate the superior accuracy of the zero-trust SMPC algorithms in identifying legitimate threats while minimizing false alarms. This improvement is consistent with the findings of Abadi et al., who highlighted the potential of machine learning models in enhancing cybersecurity defenses [7]. Furthermore, the average incident response time was reduced from 4 hours to 1 hour, which underscores the algorithms' efficiency in quickly detecting and mitigating threats.

4.3. Impact on Incident Costs and Data Protection

The financial impact of security incidents was significantly mitigated by the implementation of zero-trust SMPC algorithms. The average cost per incident decreased by 80%, and data loss per incident was reduced by 90%, demonstrating substantial financial and data protection benefits (Table 6). This aligns with the study by Chandola et al., which emphasized the cost-saving potential of effective anomaly detection systems in cybersecurity [8]. The reduction in the number of compromised records from 1,000 to 100 further highlights the enhanced data protection measures provided by the algorithms.

4.4. Compliance with Regulatory Standards

Compliance with major regulatory standards such as GDPR and CCPA improved significantly post-implementation. The GDPR compliance score increased from 70% to 95%, while the CCPA compliance score improved from 65% to 90% (Figure 3a). This improvement is crucial for SMEs, as non-compliance with these regulations can result in severe financial penalties and reputational damage. The enhanced compliance scores indicate that the zero-trust SMPC algorithms effectively address data protection requirements mandated by these regulations, aligning with the findings of Pearson and Benameur [9].

4.5. User Satisfaction and System Usability

User satisfaction and system usability scores also saw significant improvements, increasing from 60% to 85% and from 65% to 90%, respectively (Figure 3b). This positive reception highlights the ease of use and effectiveness of the new system. Improved user satisfaction is crucial for the widespread adoption of cybersecurity solutions, as user resistance can often be a barrier to effective implementation [10].

4.6. System Performance and Data Integrity

The system performance metrics indicated notable enhancements, with system availability improving from 95% to 99%, and network latency decreasing by 60% (Table 6). These improvements suggest that the zero-trust SMPC algorithms not only enhance security but also contribute to overall system efficiency and reliability. The reduction in data tampering incidents by 86.67% and the improvement in data accuracy from 85% to 99% demonstrate stronger data protection measures, ensuring the integrity and reliability of the data processed by SMEs [11].

While the findings of this study align with much of the existing literature on the benefits of zero-trust architectures and advanced machine learning models, there are some areas of divergence. For instance, the substantial reduction in the financial impact of security incidents contrasts with some studies that have reported minimal cost savings with similar implementations [12]. This discrepancy could be attributed to the specific focus on SMEs in this study, which often face higher relative costs from security breaches compared to larger organizations. The significant improvements in regulatory compliance scores also highlight a divergence from studies that have reported challenges in achieving compliance with zero-trust models due to their complexity [13]. The success in this area suggests that the tailored implementation of zero-trust SMPC algorithms can effectively address these challenges.

5. Conclusion

The deployment of zero-trust SMPC algorithms in SMEs within the U.S. supply chain has demonstrated significant improvements in cybersecurity metrics, including enhanced threat detection, reduced incident response times, and substantial mitigation of financial and data impacts. The algorithms also improved compliance with regulatory standards, user satisfaction, system performance, and data integrity. These advancements underscore the potential of zero-trust SMPC algorithms to provide robust, scalable, and economically viable cybersecurity solutions tailored to the needs of SMEs.

The benefits of this research extend beyond individual businesses to the broader U.S. economy. By enhancing the cybersecurity posture of SMEs, which form a critical component of the supply chain, the overall resilience and stability of the national economy are strengthened. This research highlights the importance of continued investment in advanced cybersecurity technologies and their tailored application to address the unique challenges faced by SMEs. The findings support the broader adoption of zero-trust SMPC algorithms as a key strategy in safeguarding the financial transactions and sensitive data of SMEs, thereby contributing to economic stability and growth in the United States.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] U.S. Small Business Administration, Office of Advocacy. (2020). 2020 Small Business Profile. Retrieved from https://www.sba.gov/document/support--small-business-profiles-states-and-territories

[2] Verizon. (2020). Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

[3] Federal Bureau of Investigation (FBI). (2020). 2020 Internet Crime Report. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[4] Kshetri, N. (2017). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

[5] Rose, S., & Borchert, O. (2020). Zero Trust Architecture. National Institute of Standards and Technology, Special Publication 800-207.

[6] Goldreich, O. (2009). Foundations of cryptography: volume 2, basic applications. Cambridge University Press.

[7] Abadi, M., et al. (2016). TensorFlow: A system for large-scale machine learning. In 12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16) (pp. 265-283).

[8] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58.

[9] Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 693-702). IEEE.

[10] Schmidt, C. G., & Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. Journal of Purchasing and Supply Management, 25(4), 100552.

[11] European Union Agency for Cybersecurity (ENISA). (2020). Guidelines for Securing the Supply Chain. Retrieved from https://www.enisa.europa.eu/publications/guidelines-for-securing-the-supply-chain

[12] Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials, 22(3), 1686-1721.

[13] Bertino, E., & Sandhu, R. (2016). Database security—concepts, approaches, and challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2-19.

[14] Kim, G., Lee, S., & Kim, S. (2019). A novel approach to monitor the security of enterprise networks using machine learning. IEEE Access, 7, 155425-155438.

[15] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication.

[16] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

[17] Keller, M., et al. (2020). MP-SPDZ: A Versatile Framework for Multi-Party Computation. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (pp. 1575-1590).

[18] Kreps, J., Narkhede, N., & Rao, J. (2011). Kafka: A distributed messaging system for log processing. In Proceedings of the NetDB (pp. 1-7).

[19] Merkel, D. (2014). Docker: Lightweight Linux containers for consistent development and deployment. Linux Journal, 2014(239), 2.

[20] Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 693-702). IEEE.

[21] Schmidt, C. G., & Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. Journal of Purchasing and Supply Management, 25(4), 100552.

[22] NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.

[23] Dhladhla, V. (2021). Enhancing Supply Chain Security through Cloud Computing. Journal of Supply Chain Management, 15(3), 45-59.

[24] Kamath, R. (2018). Food traceability on blockchain: Walmart's pork and mango pilots with IBM. The Journal of the British Blockchain Association, 1(1), 3712.

[25] Lee, J. & Lee, K. (2020). The impact of artificial intelligence on the supply chain: A review and analysis. Journal of Supply Chain Management Science, 4(2), 60-78.

[26] Marinescu, D. C. (2013). Cloud computing: Theory and practice. Morgan Kaufmann.

[27] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. Decision Support Systems, 51(1), 176-189.

[28] Goldreich, O. (2009). Foundations of cryptography: volume 2, basic applications. Cambridge university press.

[29] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication.