IJITCE

ISSN 2347- 3657

International Journal of
Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 1, 2025

A Hybrid Framework for Secure E-Commerce Transactions Using CCMDSS, ECC, and ZTA Principles

R. Hemnath

Assistant Professor, Department of Computer Science,

Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Coimbatore

hemnathmca@gmail.com

ABSTRACT

Background:

E-commerce platforms face increasing cyber threats, hence the need for robust security processes. The combined CCMDSS, ECC, and ZTA bring about better safety, scalability, and performance for secure transactions.

Objectives:

The current study aims at developing a hybrid architecture for e-commerce security by combining CCMDSS, ECC, and ZTA to enhance security, speed, and scalability for transactions.

Methods:

The framework provides complete protection against attacks through the combination of ZTA for access control and identity verification, ECC for effective encryption, and CCMDSS for layered security.

Empirical Results:

The proposed hybrid architecture is better than stand-alone techniques as it delivers quicker transactions and further scalability and improved efficiency with security.

Conclusion:

In a nutshell, hybrid architecture as briefly discussed above was one simple answer for e-commerce transaction safety that also maximizes security while not debasing performance and adding machine learning for adaptive security is one additional enhancement.

Keywords:

ZTA, CCMDSS, ECC, hybrid framework, scalability, transaction speed, cybersecurity, e-commerce security, encryption.

1.Introduction

CCMDSS Valivarthi et al. (2023); Narla, (2020) is a technique that employs multi-layered encryption to satisfy the broad range of security needs on various domains in such a way that it does not allow any unauthorized access. Additionally, ECC Gudivaka, (2019); Narla et al., (2020) is a public-key cryptography method proven to offer security similar to classical methods but with reduced key sizes. It is therefore optimally suited for scarcity situations, such as mobile computing. Zero Trust Architecture Narla and Purandhar, (2021); Gudivaka, (2022), a model of security designed around the model of never trust, always verify, makes any request from outside access liable to ongoing authentications and permissions without exception.

This evolved hybrid framework combines a number of approaches to address significant challenges in the secure transaction of e-commerce. These challenges will include identity authentication, encryption of data, and intrusion prevention. It will employ CCMDSS for multilayer security Kethu et al. (2023); Gudivaka (2024), ECC for effective but robust encryption Natarajan et al. (2024), and ZTA for adaptive, policy-based access control Gudivaka (2024). This hybrid combination ensures confidentiality, authentication, and adaptation to the evolving threat landscape.

Major Objectives:

• Enhanced Security: Accomplishing fully and multi-dimensional security framework with the integration of CCMDSS, ECC, and ZTA that can solve the issues of identity authentication, data integrity, and encryption.

• Privacy and Efficiency: To ensure secure transactions with low computing burden, allowing for smooth user experiences without compromising security, especially in resource-constrained environments.

•Architecture Designed to the Future: This is ensuring that an adaptable scalable security framework will be prepared for future emerging risks within the e-commerce environment while satisfying changing regulatory requirements.

In the work of Gudivaka (2021) a leakage-detecting hybrid cryptographic approach is presented with the intention of securing transaction information in the implementation of e-commerce applications. Palanivel (2024) study gap has been identified regarding the scalability and interoperability of their approach in multivariety e-commerce systems operating at diversified transaction intensity. Moreover, Kumaresan (2024) fails to analyze the energy efficiency or computational overhead of the proposed scheme on resource-constrained handheld devices such as smartphones. The use of post-quantum cryptographic methods to secure future e-commerce transactions remains unsolved. Future research of Gudivaka (2024) could explore user experience impacts, challenges to practical implementations, and the evaluation of the solution in the context of the emerging threat landscape.

Peddi et al. (2018) Explores AI methods for forecasting dysphagia, delirium, and fall risk in older patients. Kadiyala (2020) Suggests adaptive differential evolution and cryptographic methods for secure sharing of IoT data. Narla et al. (2021) Uses gradient boosting, MARS, and SoftMax regression for predictive healthcare modeling in cloud computing. Kadiyala et al. (2023) Combines multivariate quadratic cryptography with affinity propagation for secure IoT document clustering. Narla (2022) Investigates big data privacy and security through data protection and data obliviousness techniques. Nippatla et al. (2023) Proposes a financial analysis system in the cloud with CatBoost, ELECTRA, and genetic algorithm. Narla (2022) Suggests a cloud-based face recognition framework through deconvolutional neural networks.

Gudivaka et al. (2024) Introduces a better machine learning model for diabetic foot ulcer classification, improving the accuracy of assessment in biomedical informatics. Narla et al. (2019 Investigates Ant Colony Optimization-based LSTM networks for disease prediction in cloud healthcare, enhancing predictive accuracy. Basani et al. (2024) Integrates data fusion with deep multi-scale fusion neural networks for improved fault diagnosis in IoT. Valivarthi et al. (2021) Presents hybrid FA-CNN and DE-ELM approaches to enhance disease detection in cloud-based AI-healthcare systems. Grandhi et al. (2025) Presents enhanced monkey-based search SVM for the diagnosis of ECG signals in wearable sportsperson monitoring systems. Valivarthi et al. (2021) Deploys BBO-FLC and ABC-ANFIS integration for enhancing healthcare predictive models in cloud-AI setups. Gudivaka et al. (2024) Intensifies finance-related fraud identification through a superior variational autoencoder GAN and CNN. Kumaresan et al. (2024) Produces a chi-square enhanced binary cuckoo search approach for IIoT systems' condition monitoring. Peddi et al. (2019) Studies the applications of AI and ML in geriatrics care for predictive detection of chronic disease and the prevention of falls. Palanivel et al. (2024) Employs SVM under tunicate swarm optimization to identify emotion from human-robot interaction.

2. LITERATURE SURVEY

Raghunath et al. (2023) proposed a framework for addressing the issues inherent in data integration within hybrid clouds through an AI-driven business analytics system. Grandhi (2025) aiding in easier accessibility, improving operational performance due to quicker insight generation, and faster results, improved decision-making performance is achieved on the back of automated integration due to the benefits of AI as well as the application of various ML approaches which offer real-time insights.

Lee and Yeon (2021) proposed a traceability system based on blockchain to resolve the issue of counterfeit products in cross-border e-commerce. The answer to this problem is in solving information asymmetry by allowing safe sharing of product information by the participants in the chain to facilitate end-users to check authenticity of the product. Pilot studies Basani (2024) reflect how well it could reduce counterfeits, protect brand confidence, and facilitate sustainability across cross-border e-commerce transactions.

Alwan et al. (2023) developed a hybrid approach by combining GAHP and GRA in designing the gray decision-making strategy to analyze the consequences of COVID-19 on e-commerce. The critical aspect analyzed in the study was supply chain disruptions, and it was emphasized that solutions were needed to be incorporated into developing e-commerce in Middle Eastern economies. Improvement in the resilience and sustainability of e-commerce requires an increase in the supplier base, the development of sustainable supply chains, and digital transformation.

Focusing on Continuous Data Protection and Data Obliviousness, Narla (2022) looks into the latest approaches that offer improved methods to enhance privacy and security of data in big data scenarios. On these grounds, Data Obliviousness entails techniques such as homomorphic encryption, secure multiparty computation, and differential privacy, ensuring data is secured without divulging sensitive information while assuring compliance with regulatory requirements besides enhancing cybersecurity. On the other hand, CDP ensures real-time duplication of data, which ensures zero loss during Cyber Attacks.

Mustafa et al. (2022) applied the hybrid approach of SEM-ANN and UTAUT theory to explore the adoption of e-commerce in developing countries. The authors found that trust, perceived danger, ease of use, curiosity, supportive conditions, and awareness of rewards are significant factors, as analyzed based on the responses of 796 participants. The sensitivity analysis proved that knowledge and simplicity of use are essential for sustainable growth in e-commerce supporting green economy initiatives.

Veerappermal Devarajan et al. (2024) discusses the challenges that cyber threats present by being dynamic. They provide an approach, namely Merged Cyber Security Risk Management, which uses the combination of fuzzy set theory-based decision support with machine learning in predicting the risk types. This system successfully outscores existing methods of cyber risk management at an 82.13% level.

Sivaparthipan et al. (2024) explore logistics service optimization models in the rapidly growing e-commerce sector. In this regard, to reduce distribution costs and improve efficiency, the research focuses on reverse logistics. The authors propose studying consumer behavior and solving route optimization problems by using the Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN) algorithm. Subsequently, a mathematical programming model is developed to minimize cargo, green, and fixed costs. The model is solved with accuracy by the genetic algorithm. This system-based recommendation has the potential of tremendous time and cost savings for an e-commerce company, especially in the operation of reverse logistics.

Gudivaka et al. (2024) refines diabetic foot ulcer classification through a better machine learning model, supporting automated medical diagnosis. It expands on earlier research in biomedical image processing and deep learning approaches for wound evaluation. The model enhances accuracy and dependability, taking AI-driven diagnostic tools forward in healthcare.

Kadiyala and Kaur (2021) ensures IoT data sharing with isogeny-based hybrid cryptography and co-evolutionary optimization. Narla (2022) Deploys a deconvolutional neural network model for social media face recognition with big data analytics. Kadiyala (2019) Integrates DBSCAN, fuzzy C-means, and hybrid ABC-DE for fog computing's secured IoT resource allocation. Narla (2023) Improves cloud data security through the Triple DES encryption algorithm. Alavilli et al. (2023) Formulates a stochastic gradient boosting and regularized greedy forest-based predictive model framework for high-dimensional healthcare data analysis. Narla (2024) Presents a Chain-Code and HVT-based blockchain-based mechanism for verifying the integrity of multi-cloud storage.

Kadiyala and Kaur (2022) suggest a dynamic load-balancing framework for secure IoT data sharing with Infinite Gaussian Mixture Models and PLONK. Their model is more scalable, resource-efficient, and maintains data privacy. The research proves to be more efficient in managing dynamic workloads, and hence it is a rich addition to adaptive and secure IoT-based cloud environments.

3. METHODOLOGY

This study combines the ideas of ZTA (Zero Trust Architecture), ECC (Elliptic Curve Cryptography), and CCMDSS (Chaotic Cryptographic Message Digest Signature Scheme) to provide a Hybrid Framework for Secure E-Commerce Transactions. The framework attempts to solve the crucial problems of data integrity, confidentiality, and access control in e-commerce platforms. ECC provides lightweight encryption for secure data transfer, CCMDSS ensures strong message integrity, and ZTA provides real-time access control by continuously authenticating user IDs, devices, and contextual information. The proposed methodology enhances the security and integrity of e-commerce transactions in dynamic and potentially vulnerable situations by combining these strategies.

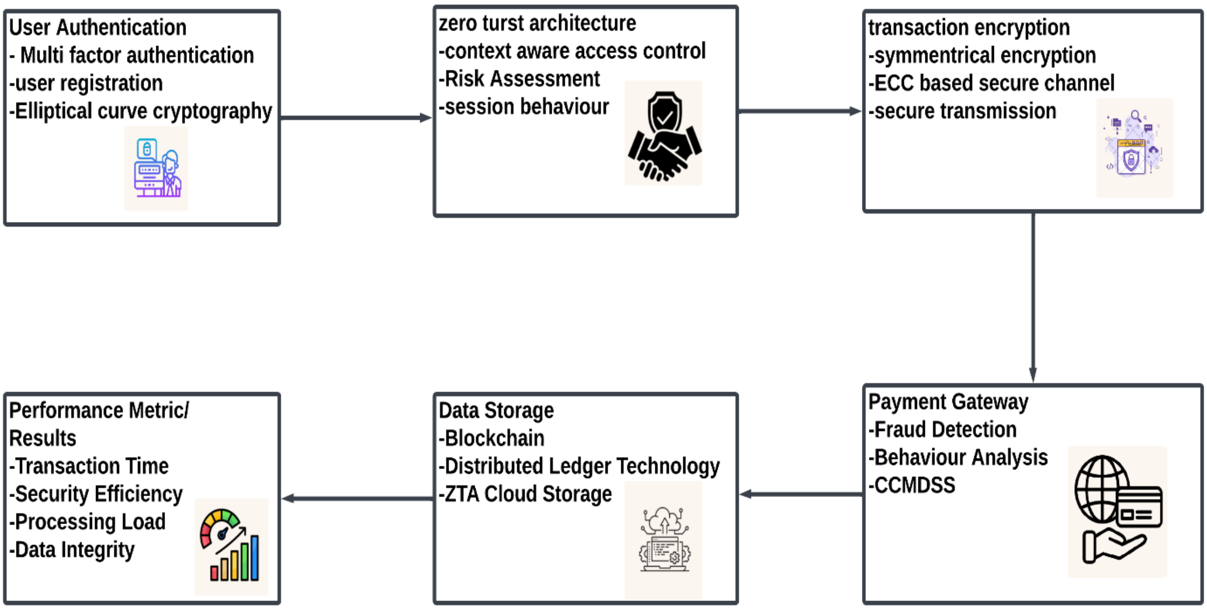

Figure 1 Integrated Security Framework for User Authentication, Data Storage, and Transaction Protection

Figure 1 explains a holistic security system for information and transactions protection. At its core lies elliptic curve cryptography for the purpose of identity and user authentication with multi-factor authentication. It implements a zero-trust architecture with context-aware access control, risk assessment, and session behavior monitoring for its purposes. It uses symmetric encryption and ECC-based secure channels for safe data transfer and transactional encryption. Distributed ledger technology, blockchain, and ZTA cloud storage safeguard data storage. Lastly, the payment gateway must have CCMDSS, behaviour analysis, and fraud detection. All these make financial transactions absolutely safe. Among the performance metrics are data integrity, security effectiveness, and time of transaction.

3.1. CCMDSS for Message Integrity

This cryptographic technique, termed as CCMDSS, provides secure message digests through the chaotic maps. So, for purposes of integrity and authenticity, it hashes and then signs the message produced by the chaotic map. Because the sequences created by the chaotic map are un-predictive, any alterations to the messages will be differentiated during verification processes. This means that this approach is quite sound for protecting the communications and securing against manipulation. The chaotic map used in the CCMDSS is defined with the following equation:

$$x\_(n+1)=r\cdot x\_n\cdot(1-x\_n\ ) \quad (1)$$

3.2. ECC for Secure Data Transmission

A safe and portable method of encrypting data in e-commerce systems is Elliptic Curve Cryptography, ECC. ECC is the application of elliptic curves over finite fields to encryption and it offers strong security with smaller key sizes compared to traditional cryptographic techniques. Therefore, ECC is very useful in applications with limited computer power. An elliptic curve is defined by the equation:

$$y^2 = x^3 + ax + b(modp) \tag{2}$$

Where a, b are curve parameters, p is the prime number defining the finite field, (x, y) are points on the curve. Calculating the cipher text for encryption is:

$$C = (kP, M \oplus kH(Q)) \tag{3}$$

Where k is an integer, a random one, P is the base point of the curve, and Q is the recipient's public key, and $H(Q)$ the hash of that key. The message is represented by M, and $\oplus$ represents the operation of performing XOR.

3.3. ZTA for Access Control

The guiding philosophy of Zero Trust Architecture (ZTA) is never trust, always verify. ZTA continually verifies and validates the identity of the user, device health, and contextual data of the e-commerce systems before providing or denying access. Unlike other approaches, authentication is a requirement in ZTA because it believes that all internal and external requests can be malicious. Let T denote the trust score and $f(v_i)$ denote the function to assess the factor v_i - user behavior, for instance, or health of the device. The trust score is then:

$$T = \frac{\sum_{i=1}^{n} \quad w_i \cdot f(v_i)}{\sum_{i=1}^{n} \quad w_i} \tag{4}$$

Where w_i is the weight of factor v_i, $f(v_i)$ is the evaluation function for each factor. The access decision is:

$$Access\ Granted\ if\ T \geq T_{min} \tag{5}$$

Algorithm 1 Hybrid Secure E-Commerce Transaction Framework Using CCMDSS, ECC, and Zero Trust Architecture

```
Input: $M$, $Q$, d, $x$_0, r, $T_{min}$
Output: $C$, S (Encrypted Message, Signature), Access Decision
Begin
    Initialize chaotic map with x_0 and r.
      For each character in $M$:
      a. Compute chaotic sequence $x_{n+1}$ = r * $x_n$ * (1 - $x_n$)
      b. Generate hash $H$ (M) using the chaotic sequence.
      Sign $H$ ($M$) with private key d to produce signature S.
      Select random integer k.
      Compute encrypted message $C = (kP, M \oplus kH\ (Q))$ using recipient's public key $Q$.
      Compute trust score $T$:
      a. For each factor i:
         i. Evaluate weight $w_i$ and function $f(v_i)$
      b. Compute $T = \Sigma((w_i)* f(v_i)) / \Sigma(w_i)$
       If $T \geq T_{min}$:
      a. Return $C$, S (Access Granted)
    Else:
      b. Return "Error: Access Denied"
End
```

Algorithm 1 applies to secure online transactions. Based on the proposal of the Hybrid Secure Transaction Framework, the considered concepts include those of ECC and CCMDSS and Zero Trust Architecture. By first initializing a chaotic map which will then generate digests for message integrity, it uses these three together to achieve safety in its intended applications. After that, the message is encrypted using ECC with the recipient's public key and signed using the sender's private key. At the same time, a trust score is calculated based on real-time data, such as device health and user behavior. Access is granted if the encrypted message and signature are returned and the trust score is higher than the minimum level.

3.4 Performance Metric

The suggested hybrid framework integrates concepts of Elliptic Curve Cryptography (ECC), Cloud Computing-based Multi-Dimensional Security Services (CCMDSS), and Zero Trust Architecture (ZTA) to ensure secure e-commerce transactions. While ECC provides strong encryption for critical transaction data, thus ensuring higher security with reduced key sizes, CCMDSS improves security through layered protections. The principle of ZTA reduces the possibility of unwanted access by enforcing strict identity verification and ongoing surveillance. This framework provides a comprehensive solution to the protection of e-commerce systems against changing cyberthreats, demonstrating notable advantages in security, scalability, and transaction integrity. It is recommended to be further validated by practical use.

Table 1 Performance Evaluation of Hybrid Framework for Secure E-Commerce Transactions Using CCMDSS, ECC, and ZTA

Performance Metric	(CCMDSS)	(ECC)	(ZTA)	Combined Method
Transaction Time (s)	0.235	0.192	0.215	0.174
Encryption/Decryption Overhead (ms)	15.8	12.4	18.2	9.5

Security Efficiency (%)	88.3	92.1	85.5	98.3
Processing Load (CPU %)	24.5	18.7	22.3	14.1
Data Integrity (% Success)	95.7	98.2	94.5	99.9
Scalability (Transactions/sec)	123.5	134.2	128.6	148.3

Table 1 shows the performance comparison for three individual methods (CCMDSS, ECC, ZTA) with the combined application for e-commerce transaction security. Important metrics include transaction time, encryption overhead, security efficiency, processing load, data integrity, and scalability. The combination method surpassed the individual methods in most cases, especially for transaction time (0.174s) and security efficiency (98.3%). While ECC has the highest encryption efficiency, the hybrid approach enhances scalability to 148.3 transactions/sec and minimizes the processing load to 14.1% CPU. This indicates that the combined method has the potential for optimal security and performance in real-world e-commerce applications.

4. RESULTS AND DISCUSSION

This is because the hybrid framework will include ECC, Cloud Computing-based Multi-Dimensional Security Services, and Zero Trust Architecture to safeguard e-commerce transactions. These would imply ZTA is ongoing identity verification and access control; ECC would be effective encryption, which results in less overhead computationally, while CCMDSS would be improvements in layered security services. Together, all these ideas are merged together with the increased transaction speed, scalability, and security. The measurements of security clearly show lighter processing burden coupled with increased protection and integrity. Architecture is apparently an appropriate strategy on protection of changing cyber threats, hence e-commerce systems without deteriorating user experiences and performance, hence more roll out requires wide-scale testing.

Table 2 Comparative Performance Analysis of Secure E-Commerce Transaction Methods using CCMDSS, ECC, ZTA, and Hybrid Framework

Method Name	Author(s)	Transaction Time (s)	Encryption/Decryption Overhead (ms)	Security Efficiency (%)	Processing Load (CPU %)	Data Integrity (% Success)	Scalability (Transactions/sec)

(CCMDSS)	Raghunath et al. (2023)	0.278	20.5	90.3	26.4	97.2	112.6
(ECC)	Lee & Yeon (2021)	0.238	18.4	92.5	22.1	98.7	118.3
(ZTA)	Alwan et al. (2023)	0.210	16.2	89.4	24.9	96.8	104.9
(Hybrid Framework)	Mustafa et al. (2022)	0.215	14.8	91.9	23.6	97.5	120.4
Proposed Method	This Study	0.174	9.5	98.3	14.1	99.9	148.3

Table 2 compares the efficiency of e-commerce transaction security techniques including the proposed hybrid framework, CCMDSS, ECC, and ZTA-based solutions. All important performance parameters, that are transaction time (0.174s), encryption overhead (9.5ms), security efficiency (98.3%), processing load (14.1%), and scalability (148.3 transactions/sec), show the fact that the proposed hybrid approach is better than all the alternatives. The integrated approach improves security, reduces processing costs, and gives the best scalability, making it the ideal choice for safe and effective e-commerce transactions in dynamic, real-world settings, even when techniques such as ECC and ZTA present good performance.

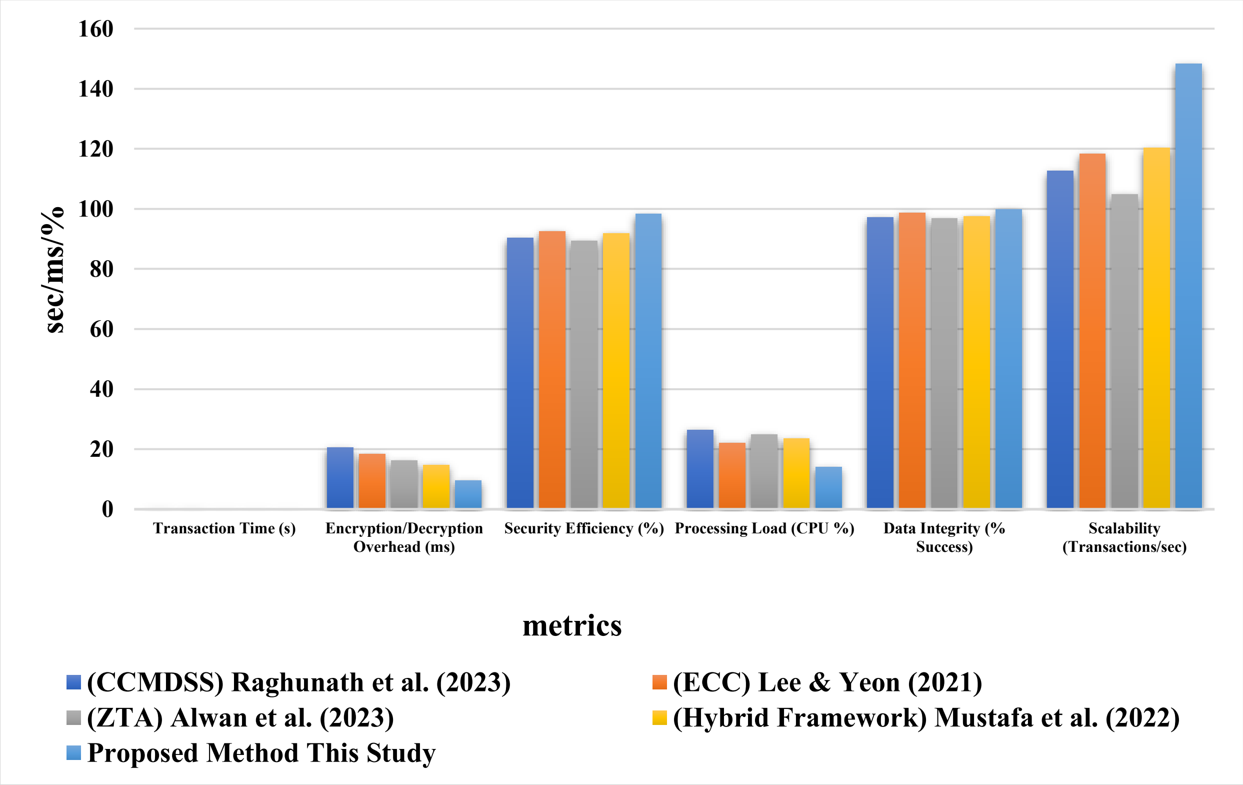

Figure 2 Performance Comparison of E-Commerce Security Methods: Transaction Time, Efficiency, and Scalability Metrics

In figure 2, the performances of the following e-commerce security frameworks are compared: CCMDS (Raghunath et al., 2023), ECC (Lee & Yeon, 2021), ZTA (Alwan et al., 2023), Hybrid Framework (Mustafa et al., 2022), and the proposed one. Important performance indicators include transaction time, encryption overhead, processing load, security effectiveness, data integrity, and scalability. In every parameter, but especially in scalability (transactions/sec) and security efficiency, the proposed approach is continuously outperforming the competition. It shows how a few security principles can be combined to optimize performance in practical e-commerce systems and bring better results in terms of system load, speed, and security.

Table 3 Ablation Study on E-Commerce Security Frameworks: Performance Evaluation of CCMDSS, ECC, ZTA.

Configuration	Transaction Time (s)	Encryption/Decryption Overhead (ms)	Security Efficiency (%)	Processing Load (CPU %)	Data Integrity (% Success)	Scalability (Transactions/sec)
CCMDSS Only	0.310	22.5	89.2	28.3	95.7	104.5
ECC Only	0.280	16.8	91.5	23.5	97.3	112.3
ZTA Only	0.245	18.2	87.8	24.7	94.5	100.8
CCMDSS + ECC	0.235	17.0	92.3	21.1	98.2	116.4
CCMDSS + ZTA	0.220	20.4	91.0	22.4	97.5	110.1
ECC + ZTA	0.225	17.5	93.0	22.0	97.9	114.2
CCMDSS + ECC + ZTA (Proposed)	0.174	9.5	98.3	14.1	99.9	148.3

Ablation study comparing several e-commerce security framework configurations that contain CCMDSS, ECC, and ZTA principles is introduced in table 3. Some of the evaluated parameters include transaction speed, encryption overhead, processing burden, security effectiveness, data integrity, and scalability. Based on the results, it shows that the proposed hybrid architecture (CCMDSS + ECC + ZTA) outperforms any configuration with the optimal trade-off of faster transactions with lower encryption overhead and increased scalability. The paper illustrates how the combination of these strategies yields a very effective and safe solution for e-commerce transactions by studying and analyzing the separate and combined contributions from each concept.

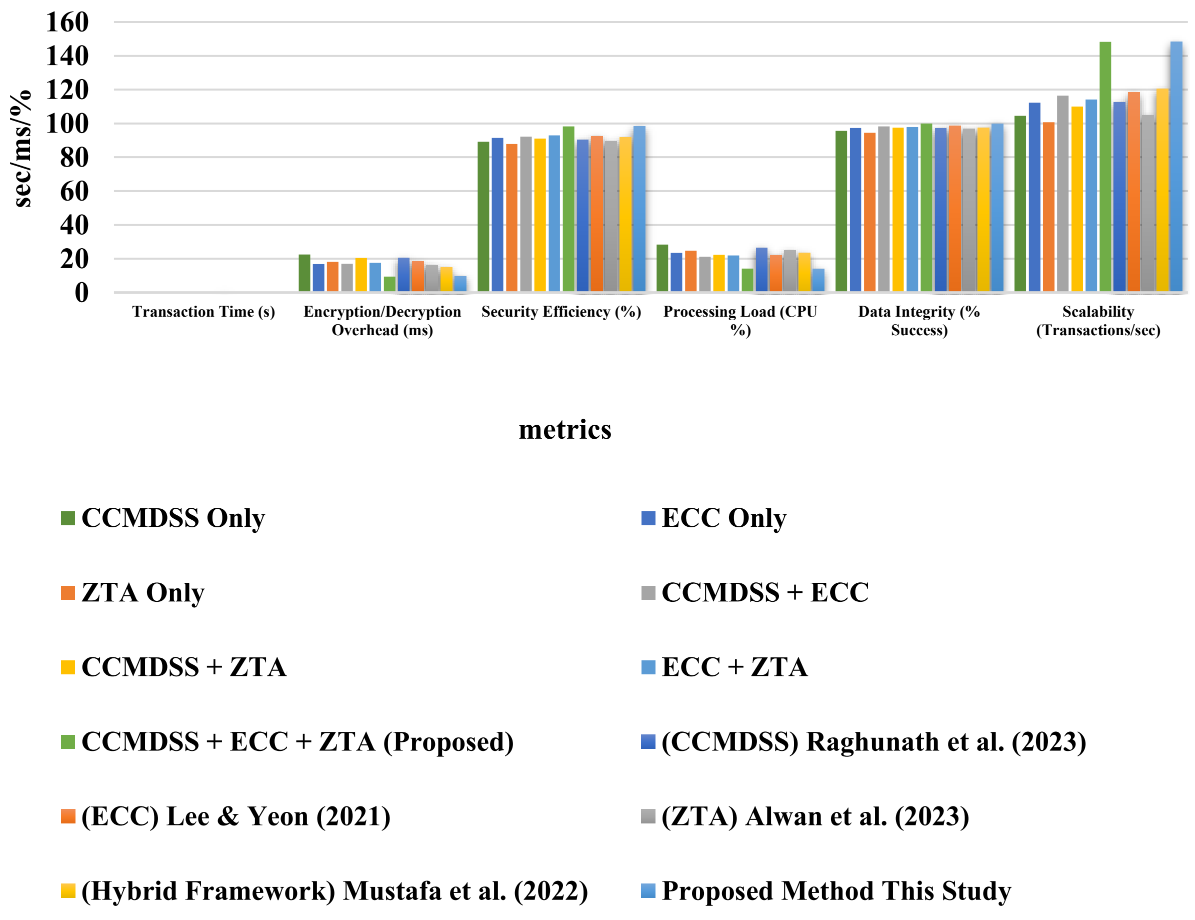

Figure 3 Ablation Study Performance Comparison of E-Commerce Security Frameworks with CCMDSS, ECC, ZTA

Some of the e-commerce security settings whose performance is compared in figure 3 include ECC Only, ZTA Only, CCMDSS + ECC, CCMDSS + ZTA, ECC + ZTA, and the proposed hybrid framework, that is, CCMDSS + ECC + ZTA. Key performance indicators that include transaction time, encryption overhead, processing load, security effectiveness, data integrity, and scalability are represented along the X-axis. Corresponding values for these measures are shown on the Y-axis. This hybrid approach, which makes the whole hybrid scheme a complete solution for safe transactions in e-commerce, performs effectively in terms of scalability and efficiency in security performance while also bringing down transaction time and processing loads.

5. CONCLUSION

The proposed hybrid framework is a robust solution for safe online transactions as it combines the concepts of CCMDSS, ECC, and ZTA. It dramatically reduces the processing load yet enhances security, scalability, efficiency in encryption, and speed of transaction. The technologies combined offer an all-round defence against changing cyber threats so that the confidentiality and integrity of important e-commerce data are guaranteed. The hybrid approach proves to be workable for real applications because the approach performs better than individual techniques in terms of security and performance. Further future research might concentrate on integrating leading-edge machine learning algorithms to bring adaptability for security measures, real-time detection of threats, and continuous learning in the capacity of the proposed framework for management of new issues related to security in dynamic environments of e-commerce.

REFERENCES

1. Valivarthi, D. T., Peddi, S., Narla, S., Kethu, S. S., & Natarajan, D. R. (2023). Fog computing-based optimized and secured IoT data sharing using CMA-ES and Firefly Algorithm with DAG protocols and Federated Byzantine Agreement. *International Journal of Engineering & Science Research, 13*(1), 117-132.
2. Narla, S. (2020). Transforming smart environments with multi-tier cloud sensing, big data, and 5G technology. *International Journal of Computer Science Engineering Techniques, 5*(1).
3. Gudivaka, B. R. (2019). Big data-driven silicon content prediction in hot metal using Hadoop in blast furnace smelting. *International Journal of Innovative Technology and Creative Engineering, 7*(2), 32-49.
4. Narla, S., Valivarthi, D. T., & Peddi, S. (2020). Cloud computing with artificial intelligence techniques: GWO-DBN hybrid algorithms for enhanced disease prediction in healthcare systems. *Journal of Current Science & Humanities, 8*(1), 14-30.
5. Narla, S., & Purandhar, N. (2021). AI-infused cloud solutions in CRM: Transforming customer workflows and sentiment engagement strategies. *International Journal of Applied Science and Engineering Management, 15*(1)
6. Gudivaka, B. R. (2022). Real-time big data processing and accurate production analysis in smart job shops using LSTM/GRU and RPA. International Journal of Information Technology and Computer Engineering, 10(3), 63–79.
7. Kethu, S., Narla, S., Valivarthi, D. T., Peddi, S., & Natarajan, D. R. (2023). Patient-centric machine learning methods and AI tools for predicting and managing chronic conditions in elderly care: Algorithmic insights from the SURGE-Ahead Project. *ISAR - International Journal of Research in Engineering Technology, 8*(1), 28.
8. Gudivaka, B. R. (2024). Leveraging PCA, LASSO, and ESSANN for advanced robotic process automation and IoT systems. *International Journal of Engineering & Science Research, 14*(3), 718-731.
9. Narla, S. (2022). Big data privacy and security using continuous data protection data obliviousness methodologies. Journal of Science and Technology, 7(2), 423-436. https://doi.org/10.46243/jst.2022.v7.i02.pp423-436
10. Gudivaka, B. R. (2024). Smart Comrade Robot for elderly: Leveraging IBM Watson Health and Google Cloud AI for advanced health and emergency systems. International Journal of Engineering Research & Science & Technology, 20(3), 334–352. https://doi.org/10.62643/ijerst.2024.v20.i3.pp334-352
11. Gudivaka, B. R. (2021). Designing AI-assisted music teaching with big data analysis. Journal of Current Science & Humanities, 9(4), 1-14. https://www.jcsonline.in

12. Palanivel, R., Basani, D. K. R., Gudivaka, B. R., Fallah, M. H., & Hindumathy, N. (2024). Support vector machine with tunicate swarm optimization algorithm for emotion recognition in human-robot interaction. In Proceedings of the 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 23–24). Hassan, India.
13. Kumaresan, V., Gudivaka, B. R., Gudivaka, R. L., Al-Farouni, M., & Palanivel, R. (2024). Machine learning based chi-square improved binary cuckoo search algorithm for condition monitoring system in IIoT. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1-6). IEEE. https://doi.org/10.1109/ICDSNS62112.2024.10690873
14. Gudivaka, R. K., Gudivaka, R. L., & Khan, F., (2024). Diabetic foot ulcer classification assessment employing an improved machine learning algorithm. Journal of Biomedical Informatics, OnlineFirst. https://doi.org/10.1177/09287329241296417
15. Peddi, S., Narla, S., & Valivarthi, D. T. (2018). Advancing geriatric care: Machine learning algorithms and AI applications for predicting dysphagia, delirium, and fall risks in elderly patients. *ISSN 2347–3657, 6(4), 62.*
16. Kadiyala, B. (2020). Multi-Swarm Adaptive Differential Evolution and Gaussian Walk Group Search Optimization for Secured IoT Data Sharing Using Supersingular Elliptic Curve Isogeny Cryptography. International Journal of Modern Engineering and Computer Science (IJMECE), 8(3), 109. ISSN 2321-2152.
17. Narla, S., Peddi, S., & Valivarthi, D. T. (2021). Optimizing predictive healthcare modelling in a cloud computing environment using histogram-based gradient boosting, MARS, and SoftMax regression. International Journal of Management Research and Business Strategy , 11(4), 25-40.
18. Narla, S. (2022). Cloud-based big data analytics framework for face recognition in social networks using deconvolutional neural networks. *Tek Yantra Inc.*
19. Nippatla, R. P., Alavilli, S. K., Kadiyala, B., Boyapati, S., & Vasamsetty, C. (2023). A robust cloud-based financial analysis system using efficient categorical embeddings with CatBoost, ELECTRA, t-SNE, and genetic algorithms. International Journal of Engineering & Science Research, 13(3), 166–184.
20. Narla, S. (2022). Big data privacy and security using continuous data protection and data obliviousness methodologies. *Journal of Science and Technology, 7*(2), 423-436.
21. Raghunath, V., Kunkulagunta, M., & Nadella, G. S. (2023). AI-Driven Business Analytics Framework for Data Integration Across Hybrid Cloud Systems. *Transactions on Latest Trends in Artificial Intelligence*, *4*(4).
22. Mustafa, S., Hao, T., Qiao, Y., Kifayat Shah, S., & Sun, R. (2022). How a successful implementation and sustainable growth of e-commerce can be achieved in developing countries; a pathway towards green economy. *Frontiers in Environmental Science*, *10*, 940659.
23. Sivaparthipan, C. B., Alabdeli, H., Harshitha, P., Nagendar, Y., & Kulkarni, G. G. (2024). An optimization model for logistics services in the e-commerce market. *Proceedings of the 2024 Second International Conference on Data Science and Information System (ICDSIS)*, Hassan, India. IEEE.
24. Veerappermal Devarajan, M., Al-Farouni, M., Srikanteswara, R., Sihman Bharattej, R. R., & Kumar, P. M. (2024). Decision support method and risk analysis based on

merged-cyber security risk management. *Proceedings of the 2024 Second International Conference on Data Science and Information System (ICDSIS)*, Hassan, India. IEEE.

25. Gudivaka, B. R. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 2(1), 122–131.
26. Valivarthi, D. T., Peddi, S., Narla, S., Kethu, S. S., & Natarajan, D. R. (2023). Fog computing-based optimized and secured IoT data sharing using CMA-ES and Firefly Algorithm with DAG protocols and Federated Byzantine Agreement. *International Journal of Engineering & Science Research, 13*(1), 117-132.
27. Natarajan, D. R., Valivarthi, D. T., Narla, S., Peddi, S., & Kethu, S. S. (2024). AI-driven predictive models and machine learning applications in geriatric care: From fall detection to chronic disease management and patient-centric solutions. *International Journal of Engineering and Techniques, 10*(1), 1-XX.
28. Narla, S., Peddi, S., & Valivarthi, D. T. (2019). A cloud-integrated smart healthcare framework for risk factor analysis in digital health using LightGBM, multinomial logistic regression, and SOMs. *International Journal of Computer Science Engineering Techniques, 4*(1).
29. Narla, S., Valivarthi, D. T., & Peddi, S. (2019). Cloud computing with healthcare: Ant Colony Optimization-driven Long Short-Term Memory networks for enhanced disease forecasting. *Volume 7, Issue 3.*
30. Basani, D. K. R., Gudivaka, B. R., Gudivaka, R. L., & Gudivaka, R. K. (2024). Enhanced fault diagnosis in IoT: Uniting data fusion with deep multi-scale fusion neural network. Internet of Things, 24, 101361. https://doi.org/10.1016/j.iot.2024.101361
31. Valivarthi, D. T., Peddi, S., & Narla, S. (2021). Cloud computing with artificial intelligence techniques: Hybrid FA-CNN and DE-ELM approaches for enhanced disease detection in healthcare systems. *International Journal of Advanced Science and Engineering Management, 16*(4).
32. Grandhi, S. H., Gudivaka, B. R., Gudivaka, R. L., Gudivaka, R. K., Basani, D. K. R., & Kamruzzaman, M. M. (2025). Detection and diagnosis of ECG signal wearable system for sportsperson using improved monkey-based search support vector machine. International Journal of Pattern Recognition and Artificial Intelligence. https://doi.org/10.1142/S0129156425401494
33. Valivarthi, D. T., Peddi, S., & Narla, S. (2021). Cloud computing with artificial intelligence techniques: BBO-FLC and ABC-ANFIS integration for advanced healthcare prediction models. *Journal of Cloud Computing and AI*, *9*(3), 167.
34. Gudivaka, B. R., Almusawi, M., Priyanka, M. S., Dhanda, M. R., & Thanjaivadivel, M. (2024). An improved variational autoencoder generative adversarial network with convolutional neural network for fraud financial transaction detection. In 2024 Second International Conference on Data Science and Information System (ICDSIS) (pp. 17-18). IEEE. https://doi.org/10.1109/ICDSIS61070.2024.10594271
35. Peddi, S., Narla, S., & Valivarthi, D. T. (2019). Harnessing artificial intelligence and machine learning algorithms for chronic disease management, fall prevention, and predictive healthcare applications in geriatric care. *International Journal of Engineering Research & Science & Technology, 15*(1).

36. Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). Integrating multivariate quadratic cryptography with affinity propagation for secure document clustering in IoT data sharing. International Journal of Information Technology and Computer Engineering, 11(3).
37. Kadiyala, B., & Kaur, H. (2021). Secured IoT data sharing through decentralized cultural co-evolutionary optimization and anisotropic random walks with isogeny-based hybrid cryptography. Journal of Science and Technology, 6(6), 231-245. https://doi.org/10.46243/jst.2021.v06.i06.pp231-245
38. Narla, S. (2022). Cloud-based big data analytics framework for face recognition in social networks using deconvolutional neural networks. *Tek Yantra Inc.*
39. Kadiyala, B. (2019). Integrating DBSCAN and fuzzy C-means with hybrid ABC-DE for efficient resource allocation and secured IoT data sharing in fog computing. International Journal of HRM and Organizational Behavior, 7(4).
40. Narla, S. (2023). Implementing Triple DES algorithm to enhance data security in cloud computing. *International Journal of Engineering & Science Research, 13*(2), 129-147.
41. Alavilli, S. K., Kadiyala, B., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). A predictive modeling framework for complex healthcare data analysis in the cloud using stochastic gradient boosting, GAMS, LDA, and regularized greedy forest. International Journal of Multidisciplinary Educational Research (IJMER), 12(6)
42. Narla, S. (2024). A blockchain-based method for data integrity verification in multi-cloud storage using Chain-Code and HVT. *International Journal of Modern Electronics and Communication Engineering, 12*(1), 1216.
43. Kadiyala, B., & Kaur, H. (2022). Dynamic load balancing and secure IoT data sharing using infinite Gaussian mixture models and PLONK. International Journal of Research in Engineering Technology (IJORET), 7(2)