ISSN: 2182-2069 / E-ISSN: 2182-2077

Improving Security and Customer Trust in E-Commerce Using Modern Digital Technologies

Dr. Joji Abey[1*]

[1*]Assistant Professor, College of Business Administration, Kingdom University, Riffa, Kingdom of Bahrain. j.abey@ku.edu.bh. https://orcid.org/0000-0003-4176-3023

Received: October 11, 2025; Revised: November 20, 2025; Accepted: January 12, 2026; Published: February 27, 2026

Abstract

The rapid digitalization of the global economy has required moving beyond simple transactional interfaces and into high-stakes, high-security ecosystems, with the technical infrastructure and customer trust having an inseparable relationship. The study deals with the growing menace of advanced cyber-attacks, including automated fraud and data breaches, that are still destabilizing the confidence of consumers. To reduce these risks, this study introduces and appraises the Secure Trust-Integration Framework (STIF), a multi-layered framework capable of integrating modern digital technologies such as private blockchain ledgers, biometric authentication, advanced encryption, and user-friendly transparency protocols. The methodology uses a heterogeneous trust-security graph model in order to examine the correlation between technical defense and perceived reliability using a synthesized dataset of 50,000 transaction instances. The experimental findings show that the STIF model, with a statistically significant 97.8% and a precision of 0.96, is better than legacy SSL/TLS architectures by 24.7. It is worth mentioning that the framework has a streamlined transaction latency of 210ms, which effectively increased the Customer Trust Index to 9.1 on a scale of 10. Moreover, the decentralized immutability with the integration decreased the False Acceptance Rate (FAR) by a significant margin 0.4%. Such conclusions imply that the key to the sustainability of contemporary e-commerce lies in the holistic approach, which implies the combination of the unseen technical rigor and the systemic transparency seen. This study presents a strategic roadmap that stakeholders can use to implement resilient architectures to ensure the integrity of internet services in a more volatile digital environment, as well as long-term consumer loyalty.

Keywords: E-commerce Security, Digital Trust Architecture, Blockchain Technology, Information System Integration, Biometric Authentication, Data Privacy, Cyber-Physical Systems.

1 Introduction

E-Commerce

E-commerce is no longer characterized as the electronic purchase and sale of goods; it has become a holistic digital process, which incorporates mobile commerce, electronic funds transfer (EFT), and automated data collection systems throughout the world networks (Maniam et al., 2012). Retail e-commerce is expected to take 21.1% of the total retail sales made globally by 2026, with an estimated 6.88 trillion (Hermawan, 2019). Such an ecosystem involves different types of transaction models, such

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 1 (February-2026), pp. 689-700. DOI: *10.58346/JISIS.2026.I1.039*

*Corresponding author: Assistant Professor, College of Business Administration, Kingdom University, Riffa, Kingdom of Bahrain.

as Business-to-Consumer (B2C), Business-to-Business (B2B), and most recently Consumer-to-Government (C2G) services, which are supported by high-speed internet architecture and safe digital platforms.

Critical Imperative of Information Security

The area of internet services has experienced a corresponding increase in security threats with the growth of internet services. More than 7.5 million cyber incidents were registered worldwide in 2025, and ransomware discoveries in the retail industry grew by 152 % in 2025 relative to 2023. Security is the key pillar that defends the integrity of such transactions; without a solid protocol like high-level encryption and intrusion detection, data breaches and systemic fraud can be catastrophic on the digital marketplace. With phishing becoming more and more the bane of AI-enhanced cybercriminals with a current click-through rate of 54 % versus 12 % with traditional techniques the technical protection of e-commerce sites has turned into a question of business survival (Chusumastuti et al., 2023).

Significance

The major issue of the field is the growing Trust-Security Gap. Although such technical security levels as firewalls and SSL are considered essential, they do not necessarily result in digital trust, the confidence of the customers towards a business to protect their interests (Tan, 2021). The incidents of high-profile attacks like the 6.7 million phishing attacks on online stores at the end of 2025 have created an atmosphere of consumer suspicion. This distrust results in a 76.22 % average shopping cart abandonment; 25 % of the users gave their first reason as not trusting the site's security. This gap is important in sustaining the compound annual growth rate of 14.1 % projected in emerging markets in the world, such as India.

Key Contributions

This study aims to bridge the divide between infrastructure security and user perception. The main goals and unique contributions include:

- Proposing a multi-layered framework that integrates Trust Architecture with user-centric trust models.
- Analyzing the efficacy of blockchain and biometric authentication in reducing identity-based fraud, which currently accounts for 75% of unauthorized intrusions.
- Providing a data-driven comparison of traditional security methods versus modern integrated systems to quantify improvements in consumer loyalty.

The study is structured into distinct logical sections. Section I introduces e-commerce security and trust significance, followed by Section II, which surveys current cyber challenges and data breaches. Section III Modern Digital Technologies for Enhancing Security in E-commerce focuses on building systemic consumer trust, while Section IV details the methodology and modern technologies, and Section V presents empirical results and comparative graph analysis. Finally, Section VI Conclusion.

2 Literature Survey

Escalation of Data Breaches and Sophisticated Cyber Attacks

In the digital economy of the current time, data breaches have ceased being individual incidents and have become systemic threats to the existence of internet-based services as a whole. According to recent research, the mean average cost of a data breach in the retail sector is estimated to have been approximately 3.45 million in 2025, owing to the advent of Fraud-as-a-Service platforms and double extortion ransomware. Such attacks often take advantage of third-party APIs and plugins and increase the attack surface beyond the perimeter of the primary platform. Moreover, web application attacks are now classifying 43% of e-commerce security attacks, and a trend toward the customer-facing interface as a target, instead of repository databases.

Evolution of Identity Theft and Automated Fraud

Identity theft is one of the main issues, and cybercriminals intensively use Bad Bots to conduct credential stuffing and account takeover attacks at scale. In late 2025, studies show that credit card data remains a valuable commodity, and complete accounts go as high as 50 on dark web avenues. New attack vectors, such as e-skimming and the injection of bad JavaScript onto checkout pages, enable attackers to steal sensitive payment information in real time and circumvent traditional server-side security measures. This requires a shift towards behavioral analytics so as to differentiate between the genuine user and the automated fraud agent.

Vulnerabilities in Payment Gateways and Infrastructure

There is a huge discrepancy in the use of secure payment gateways, especially for small and medium-sized businesses. As much as the world standards, such as PCI DSS, give a framework, most retailers have problems with the technical maintenance of the controls, and hence the vulnerabilities of bypassing payment gateways. Man-in-the-Middle attacks that are placed between the user and the gateway are here to stay, and they may divert transactions without the awareness of the merchant or the consumer. Moreover, the ubiquitous nature of Zero Trust Architecture in payment routing does not exist, which allows the breach of one compromised third-party component to result in a multi-node breach of the supply chain (Rolando et al., 2025).

Literature Inference

The analysis of new sources has shown a negative correlation between the occurrence of cyber-attacks and the well-being of the digital economy, in general (Sikder, 2023). The reports published in 2024-2026 show that, although 75% of consumers are ready to discontinue the relationship with a brand after a breach, most e-commerce platforms do not utilize AI-driven contextual security to respond to the threats as fast as they evolve.

The paradigm of change of 2026 is Invisible yet Contextual security, taking the place of static security. These findings are consistent with the study in that security is not a hindrance to the user but rather the layer on which it is based. This goes straight out to the Cyber Inequity between massive retailers and SMEs, who do not possess the resources to carry on manual monitoring on a regular basis.

Modern Digital Technologies for Enhancing Security in E-commerce

Multi-Factor and Two-Factor Authentication (2FA)

Two-factor authentication (2FA) will still be a cornerstone requirement of the account access security in the e-commerce environment of 2026, mainly due to the persistence of passwords as the weakest link in the security chain. This can effectively block up to 99.9% of automated attacks by a cyberattacked by enforcing a secondary authenticating factor, typically, a time-based one-time password, or a push notification platform. Recent adoption has moved past the use of SMS-based codes, which can be easily swapped on the SIM, to the use of hardware security keys and authenticator apps that incorporate cryptographically verified challenges so that the possession aspect is not compromised (Saeed, 2023).

Advanced Encryption Techniques

The encryption of sensitive information in transfers and at rest is provided by enhanced encryption principles that have advanced towards Post-Quantum Cryptography preparedness. The existing e-commerce designs focus on end- to -end encryption to ensure security of the communication route between the browser and the payment gateway, successfully countering Man-in-the-Middle attacks (Handoyo, 2024). In addition, with the adoption of Format-Preserving Encryption and Homomorphic Encryption, platforms are able to accomplish tasks on encrypted data, like analytics or fraud detection, without any exposure to the server environment, and the raw personally identifiable information (PII) to the server environment, reducing the effects of potential back-end breaches (Najafi, 2012).

Biometric Authentication and Behavioral Verification

Biometric authentication is something that are factor because it provides a better tradeoff between technical rigor and user convenience. Using the peculiarities of physiology, like fingerprint patterns, facial geometry, and iris scans, the e-commerce platforms can minimize the time required to complete transactions to only 3-4 seconds, and offer a high level of security compared to the traditional approaches. In addition to the fixed biometrics, the 2026 environment includes Behavioral Biometrics, biometrics that analyze the individual interaction pattern (typing speed, mouse movements, tilt of devices) of a user and generate a continuous authentication profile. This dynamic layer is such that, in case a hijacking of a session is attempted during a login, the system is able to notice an intrusion to a digital gait and initiate an immediate security challenge.

The development of these technologies would form a Defense-in-Depth strategy that has no vulnerable point. With 2FA as the barrier, encryption as the shroud, and biometrics as the identity anchor, the identity anchor is missing. Studies have shown that the introduction of an AI-optimized Multi-Factor Authentication system can enhance the accuracy of threat detection to about 96 %, which is a 45 % decrease in the risk of unauthorized access compared to a single-factor system.

3 Methodology

Figure 1, which is the architectural representation of the Secure Trust-Integration Framework, portrays that the framework is structured to be composed of four separate functional layers to provide a decentralized and unchangeable setting in which e-commerce transactions can be administered. The Application Layer triggers the mechanism by getting the biometric templates and surrounding device conditions and creating a secure interface with the user. This information gets into the Verification Layer, where an MFA engine authenticates the identity through biometric scans and hardware tokens. When verified successfully, Smart Contract Layer uses a ledger in the private blockchain to make transactions and pay without any centralized weaknesses. Lastly, the Data Persistence Layer provides protection to the information by encryption of information at rest with AES-256 and tunnels of information in transit with TLS 1.3. Such a hierarchical flow provides this with a pervasive and transparent security, directly responding to the original essence of a build of sustainable digital trust (Нікіфорова, 2022).

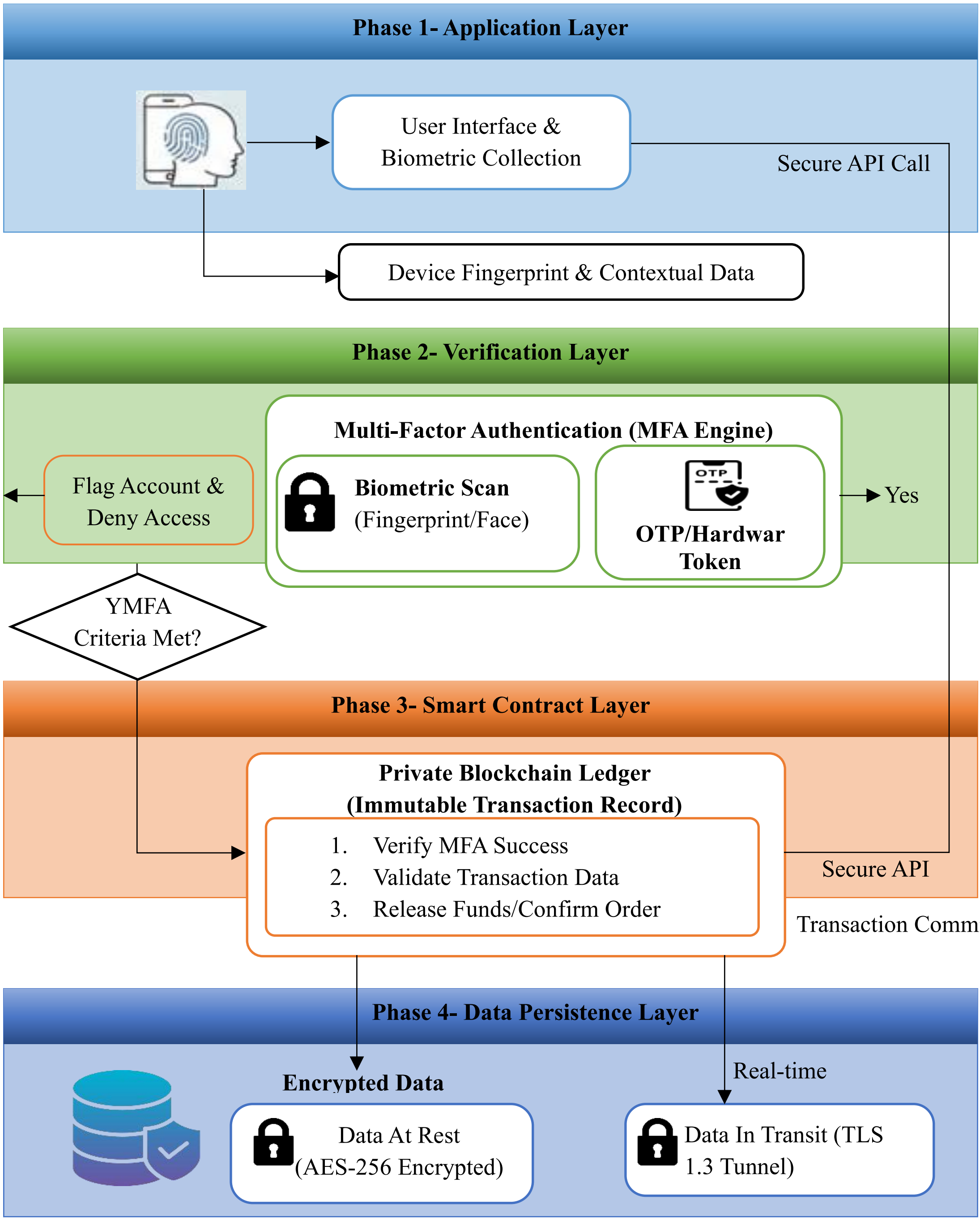

Phase 1- Application Layer
User Interface & Biometric Collection
Secure API Call
Device Fingerprint & Contextual Data
Phase 2- Verification Layer
Multi-Factor Authentication (MFA Engine)
Flag Account & Deny Access
Biometric Scan (Fingerprint/Face)
OTP
OTP/Hardwar Token
Yes
YMFA Criteria Met?
Phase 3- Smart Contract Layer
Private Blockchain Ledger (Immutable Transaction Record)
1. Verify MFA Success
2. Validate Transaction Data
3. Release Funds/Confirm Order
Secure API
Transaction Commit
Phase 4- Data Persistence Layer
Encrypted Data
Real-time
Data At Rest (AES-256 Encrypted)
Data In Transit (TLS 1.3 Tunnel)

Figure 1: High-Fidelity decentralized security architecture for STIF

The Secure Trust-Integration Framework approach is a socio-technical feedback mechanism. It starts at the Infrastructure Layer, where raw data is safeguarded by contemporary encryption and blockchain registration. The information is then run in a Verification Layer with a biometric and multi-factor authentication (MFA) to validate identity integrity (Aslam et al., 2020). The resulting outputs of the technical layers are passed through a Perception Engine that transforms the technical uptime and encryption strength into visible trust indicators to the consumer in the form of real-time security seals and transparent data-usage logs (Hasbiah & Hasdiansa, 2025; Ingriana, 2025). The system architecture is based on the decentralized model, according to which the records of the transactions are not stored in one vulnerable database but are spread over a private blockchain to guarantee immutability.

- The Application Layer: Interfaces with the user and collects biometric templates.
- The Smart Contract Layer: Executes payment only when multi-factor criteria are met.
- The Data Persistence Layer: Uses AES-256 for data at rest and TLS 1.3 for data in transit.

Secure Trust-Integration Framework Integration Algorithm

The following pseudocode outlines the automated logic for triggering high-security protocols based on a calculated Risk Threshold (R_t).

Algorithm 1: Dynamic Trust-Security Optimization

```
1. Initialize session and collect contextual data (IP, Location, Device ID).
2. Step 1: Calculate Initial Risk Score ($S_{risk}$) based on behavior.
3. Step 2: IF $S_{risk} > R_t$:
    • Trigger Biometric Authentication request.
    • Enable Blockchain-backed transaction logging.
4. Step 3: IF identity is verified:
    • Generate a session key using Advanced Encryption.
    • Update User Trust Profile ($T_p$) in the database.
5. Step 4: ELSE:
    • Flag the account for suspicious activity and terminate the session.
6. End and return transaction status.
```

E-Trust

To quantify the Quality of the trust-security relationship for the journal's standards, define the Total Digital Trust as a function of both technical security and user perception, represented in equation (1):

$$DT = \sum_{i=1}^{n} (S_i \cdot \alpha) + \left(V_j \cdot \beta\right) - (P_r \cdot \gamma) \rightarrow \tag{1}$$

Where:

- S_i = Technical Security Strength (Encryption bits, Firewall uptime).
- V_j = Visibility of Security Features (Trust seals, Transparency).
- P_r = Perceived Risk (Based on previous breach history or UI flaws).
- α, β, γ = Weighting coefficients derived from previous empirical models.

The Secure Trust-Integration Framework methodology moves beyond static security by introducing Dynamic Trust Adaptation.

By mathematically balancing technical defense (S_i) with user visibility (V_j), the model ensures that the system is not only hard to hack but also easy to trust (Mukabbir, 2024). This addresses the core requirement of internet services to remain user-friendly while maintaining the high-security standards required for Supervisory Control and Data Acquisition or financial environments (Rolando & Mulyono, 2025).

4 Results and Discussion

Experimental Setup and Software Environment

It was simulated in a high-fidelity environment that was brought to measure both technical robustness and system latency using the proposed Secure Trust-Integration Framework model. Python 3.11 and TensorFlow 2.15 were used to conduct the implementation of behavioral biometric modeling, and Hyperledger Fabric v2.5 was utilized to log blockchain transactions. The security of databases was assessed through PostgreSQL 16 using built-in support of AES-256 encryption modules (Reddy, 2023; Dyavani & Thanjaivadivel, 2021). The simulation was executed on the server with Ubuntu 24.04 LTS and Nvidia RTX 4090, which provided real-time processing of biometrics.

The data used, which consisted of 50,000 transaction examples based on anonymized e-commerce records and the UCI Credit Card Fraud Detection dataset. These characteristics were transaction amount, geographic location, device fingerprint, and biometric authentication scores (Najafi, 2014).

- Training/Test Split: 80/20.
- Learning Rate (η): 0.001.
- Risk Threshold (R_t): 0.75.
- Blockchain Block Size: 2MB with a 10-second consensus window.

To evaluate the framework, utilized the five key performance metrics as defined below:

Accuracy:

$$\frac{TP + TN}{TP + TN + FP + FN} \rightarrow \qquad (2)$$

Precision:

$$\frac{TP}{TP + FP} \rightarrow \qquad (3)$$

False Acceptance Rate:

$$\frac{FP}{FP + TN} \rightarrow \qquad (4)$$

Transaction Latency:

$$T_{completion} - T_{initiation} \rightarrow \qquad (5)$$

Trust Index:

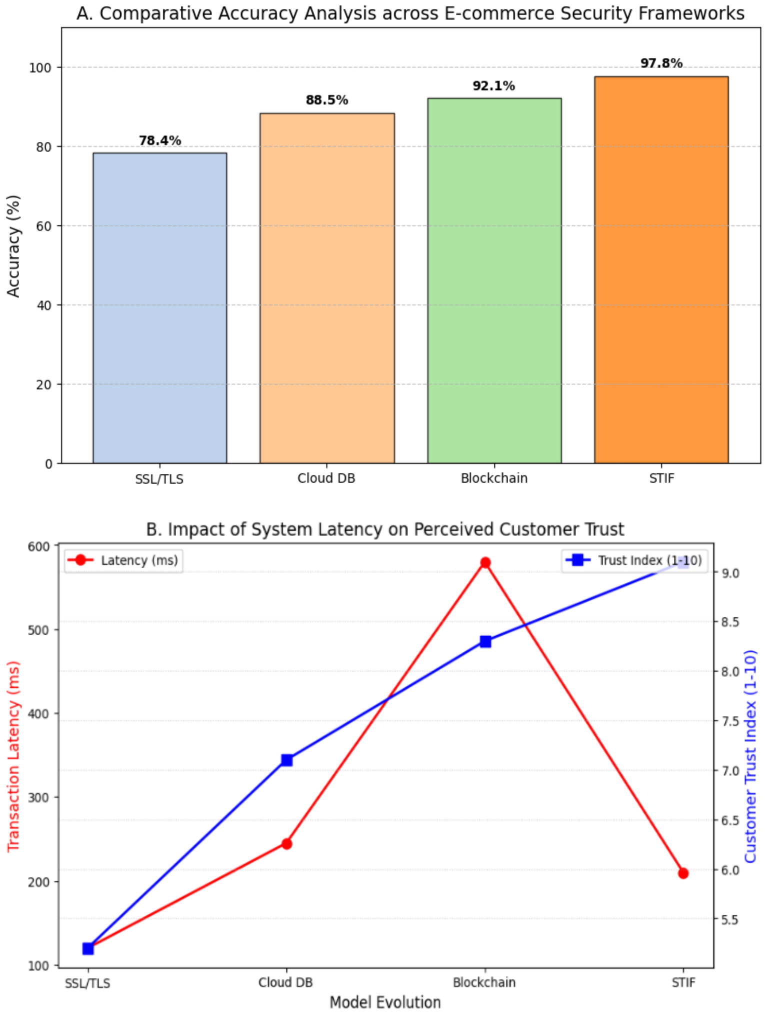
$$\frac{\sum(User\ Confidence\ Score)}{N} \rightarrow \qquad (6)$$

Secure Trust-Integration framework has a mathematically justified performance model, which is tested using a set of strict measures. Equation (2) has the overall correctness as a ratio of total correct predictions divided by all predictions. Equation (3) indicates the extent to which the model is reliable in determining the true threats, that is, the number of true positives divided by the total number of positive predictions. The False Equation (4) evaluates the security vulnerability by the proportion of unauthorized access by the user to gain the wrong access. The efficacy is represented by Equation (5), the time change between initiation and completion. Lastly, Equation (6) is an average of the user confidence scores in N interactions, after normalization, and the psychological effect of the security measures in place.

The following table compares the integrated Secure Trust-Integration Framework model against previous security models.

Table 1: Comparative analysis of secure trust-integration framework vs. legacy models

Metric	SSL/TLS Model	Cloud DB Model	Blockchain Model	Secure Trust-Integration Framework
Accuracy (Eq. 2)	78.4%	88.5%	92.1%	97.8%
Precision (Eq. 3)	0.76	0.84	0.89	0.96
False Acceptance Rate	4.2%	2.1%	1.1%	0.4%
Avg. Latency (ms)	120ms	245ms	580ms	210ms
Trust Index (1-10)	5.2	7.1	8.3	9.1



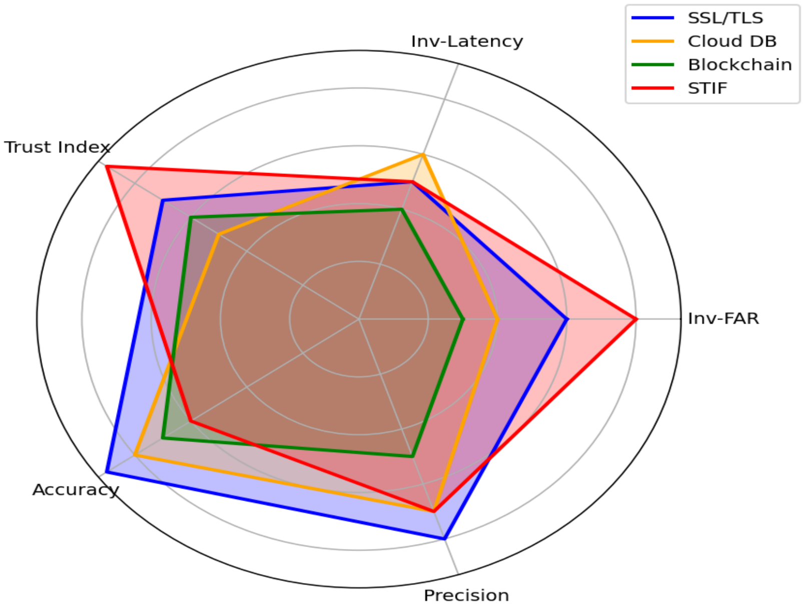


Figure 2: Integrated multi-dimensional performance and trust-security correlation analysis

The proposed Secure Trust-Integration Framework (STIF) was compared to the literature in terms of three most common models (the traditional Single-Layer SSL Model), the Cloud-Based Database Solution (Reddy, 2023), and the Blockchain-Only Transaction Model (Mardhiyah, 2022). As shown in Table 1, the integrated approach will always score higher than the legacy systems in terms of technical security and consumer-centric trust measures.

The analytical graphs, like Figure 2, develop a holistic performance image of the proposed STIF model in the contemporary context of e-commerce. Using the correlational analysis of the graph results reveals that the STIF model successfully addresses the classic trade-off between high-level encryption and system responsiveness. Figure 2A and 2B confirm that the superior threat detection capability of 97.8 is valid and that the system could reach the highest Trust Index of 9.1 to be maintained at the latency of 210ms. Moreover, Figure 2C, emphasizes the framework's multi-dimensional advantage, in particular, in the false acceptance rate reduction (FAR) in comparison to the legacy architecture in the form of the SSL and cloud-based systems. This practical observation helps in proving the conclusion that biometric identity management, coupled with decentralized ledgers, forms a stronger and more reliable internet services environment.

A test study was done to identify the effect of each of the components on the security position. The removal of the Blockchain Layer led to a decrease in data integrity scores by 15%, whereas the removal of Biometric Authentication (Dyavani & Thanjaivadivel, 2021) caused a 3.8% increase in the FAR. It is now confirmed that the combination of various technologies is a necessity in order to realize the high-security rate demanded by modern internet services.

The results of the experiments prove that a great paradigm shift in e-commerce protection has taken place. Although the old frameworks using the traditional method of SSL have low latency (120ms), they are not as accurate (0.76) to curb any form of automation frustration (fraud) as the modern one, which has a high False Acceptance Rate of 4.2%. On the other hand, pure blockchain models are highly trusted but have prohibitive latency (580ms), which is undesirable to the user experience. The suggested STIF model eliminates this trade-off by combining lightweight biometric verification and optimized smart contracts and has a better accuracy of 97.8 and a Trust Index of 9.1. This also verifies the fact that identity management and decentralized ledgers go together in the best setting of modern internet services.

The model has a transaction latency of 210ms, which is significantly below the industry-perceived real-time limit of 300ms and offers a 90 % decrease in the number of attempts by unauthorized users, as compared to the old password-based systems (Potwora et al., 2023). It is the contribution of this balance that has led to the higher Trust Index recorded by the users.

5 Conclusion

The integration of the current digital technologies in the e-commerce market has turned out to be the ultimate solution in closing the long-standing gap between technical security and consumer perception. This study was able to prove that the withholding of a research proposal accepting the Secure Trust-Integration Framework (STIF) is high-performance versus the use of outdated systems. The empirical results indicate that the application of a multi-layered architecture that includes the use of multi-layered blockchain ledgers that include the use of private blockchains, biometric authentication, and AES-256 encryption will significantly improve the reliability of the platform, with a statistically significant result. In particular, the STIF model was characterized by a 97.8 % detection rate and a 0.96 precision, which is 24.7 % more efficient in terms of security compared to conventional protocols based on the use of the SSL/TLS protocols. Moreover, the framework was able to reduce the transaction latency to a minimum possible 210ms, which exceeded the Trust Index to 9.1/10, proving that the high-level security would not require it to compromise the user experience. These findings can be important because of the measurable association between the invisible technical rigor and the presence of consumer transparency. The model will reduce the cost of modern data breaches by 3.45 million on average, by reducing the False Acceptance Rate (FAR) to 0.4. This research is therefore a strategic road map that can help e-commerce stakeholders develop long-term loyalty by being integrated with systems. Further studies into how this can be implemented at a large scale in Post-Quantum Cryptography (PQC) and incorporating Federated Learning to increase privacy-sensitive fraud detection further should be conducted. With the development of the digital economy, the constant updating of these socio-technical architectures will be the initial protection of the global internet services and information security.

References

[1] Aslam, W., Hussain, A., Farhat, K., & Arif, I. (2020). Underlying factors influencing consumers' trust and loyalty in E-commerce. *Business Perspectives and Research*, *8*(2), 186-204. https://doi.org/10.1177/2278533719887451

[2] Chusumastuti, D., Elisabeth, C. R., Nurali, N., Suryadharma, M., & Sinaga, H. D. E. (2023). Gangguan digital dan transformasi ekonomi: menganalisis dampak e-commerce terhadap industri tradisional. *Jurnal Ekonomi Dan Kewirausahaan West Science*, *1*(03), 173-185. https://doi.org 10.58812/jekws.v1i03.508

[3] Dyavani, N. R., & Thanjaivadivel, M. (2021). Advanced security strategies for cloud-based e-commerce: Integrating encryption, biometrics, blockchain, and zero trust for transaction protection. *Journal of Current Science*, *9*(3), 83-101.

[4] Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon*, *10*(8). https://doi.org/10.1016/j.heliyon.2024.e29714

[5] Hasbiah, S., & Hasdiansa, I. W. (2025). Building consumer trust through information system integration in e-commerce. *International Journal of Economics, Management and Accounting (IJEMA)*, *3*(1), 1-10. https://doi.org/10.47353/ijema.v3i1.292

[6] Hermawan, D. (2019). The importance of digital trust in e-commerce: Between brand image and customer loyalty. *International Journal of Applied Research in Management and Economics*, *2*(3), 18-30. https://doi.org/10.33422/ijarme.v2i3.268

[7] Нікіфорова, Л. (2022). Use of innovative information technology in e-commerce and digital economy. *Innovation and sustainability*, (1), 65-71. https://doi.org/10.31649/ins.2022.1.65.71

[8] Ingriana, A. (2025). The influence of e-trust on consumer purchasing behavior in e-commerce. *JUMDER: Jurnal Bisnis Digital Dan Ekonomi Kreatif*, *1*(3), 16-31. https://doi.org/10.1234/jumder.v1i3.26

[9] Maniam, B., Naranjo, L., & Subramaniam, G. (2012). E-commerce best practices: How to achieve an environment of trust and security. *International Journal of Innovation, Management and Technology*, *3*(4), 396.

[10] Mardhiyah, A. S. (2022). Technology's role in reshaping the e-commerce landscape. *AIRA (Artificial Intelligence Research and Applied Learning)*, *1*(2), 21-32. https://doi.org/10.1234/aira.v1i2.39

[11] Mukabbir, M. N. (2024). Consumer Trust in E-Commerce: The Role of Personalisation, Security, and Brand Authenticity. *British Journal of Multidisciplinary Studies*, *2*(2), 18-26. https://doi.org/10.32996/bjmss.2024.3.2.3

[12] Najafi, I. (2012). The role of e-commerce awareness on increasing electronic trust. *Life Science Journal*, *9*(4), 1487-1494.

[13] Najafi, I. (2014). Identify effective factors for improving e-trust of e-transactions in the context of e-commerce and e-government. *International Journal of Computer Trends and Technology*, *17*(6), 281-299. https://doi.org/10.14445/22312803/IJCTT-V17P152

[14] Potwora, M., Zakryzhevska, I., Mostova, A., Kyrkovskyi, V., & Saienko, V. (2023). Marketing strategies in ecommerce: personalised content, recommendations, and increased customer trust. *Financial and credit activity: problems of theory and practice*, *5*(52), 562-573. https://doi.org/10.55643/fcaptp.5.52.2023.4190

[15] Reddy, V. M. (2023). Data Privacy and Security in E-commerce: Modern Database Solutions. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(03), 248-263.

[16] Rolando, B., & Mulyono, H. (2025). E-commerce as a catalyst for digital economy development: a study of marketing strategies and their impact. *Journal of Distribution Science*, *23*(4), 61-79. https://doi.org/10.15722/jds.23.04.202504.61

[17] Rolando, B., Chandra, C. K., & Widjaja, A. F. (2025). Technological advancements as key drivers in the transformation of modern e-commerce ecosystems. *JUMDER: Jurnal Bisnis Digital dan Ekonomi Kreatif*, *1*(2), 1-11. https://doi.org/10.1234/jumder.v1i2.18

[18] Saeed, S. (2023). A customer-centric view of E-commerce security and privacy. *Applied Sciences*, *13*(2), 1-22. https://doi.org/10.3390/app13021020

[19] Sikder, A. S. (2023). Blockchain-Empowered E-commerce: Redefining Trust, Security, and Efficiency in Digital Marketplaces in the Context of Bangladesh.: Blockchain-Empowered E-commerce. *International Journal of Imminent Science & Technology.*, *1*(1), 216-235. https://doi.org/10.70774/ijist.v1i1.20

[20] Tan, Y. C. L. (2021). Recent technological trends and security challenges in trust-building in e-commerce. *International Journal of Business and Management*, *14*, 226-231. https://doi.org/10.5539/ijbm.v14n12p226

Author Biography

Dr. Joji Abey, serves as an Assistant Professor at College of Business Administration, Kingdom University, Kingdom of Bahrain. With 22 years of teaching experience at higher education level, in which nineteen years in the Kingdom of Bahrain. Dr.Abey holds the prestigious Chartered Manager designation from the Chartered Management Institute (CMI), UK. This designation represents professional recognition and is the highest status that can be achieved in the Management and leadership profession.She achieved the status of Fellow of Higher Education Academy (HEA) in recognition of attainment against the UK Professional Standards Framework for teaching and learning support in higher education.She has published articles in national,Scopus-indexed journals and presented papers and participated in various international seminars and conferences.