wjert, 2025, Vol. 11 Issue 5, 169-184 Original Article ISSN 2454-695X

World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 7.029

BLOCKCHAIN-POWERED PROTECTION AGAINST SOCIAL ENGINEERING IN E-COMMERCE

Sharmin Akhter Jui[1*], Md. Iftekhar Uddin Khan[2] and Arnab Shikder[3]

[1,2]Lecturer, Department of Computer Science and Engineering, Alhaz Mockbul Hossain College, Plot# 08 Road# 01, Kadarabad Housing Society Ltd, Mohammadpur, Dhaka- 1207, Bangladesh.

[3]Lead Infrastructure Engineer, Euro Foods Group, Navana Oval, 7th Floor, Plot# 05, Sonargaon Janapath Road, Sector# 07, Uttara, Dhaka, Bangladesh.

Article Received on 08/03/2025 **Article Revised on 28/03/2025** **Article Accepted on 17/04/2025**

***Corresponding Author**
Sharmin Akhter Jui
Lecturer, Department of Computer Science and Engineering, Alhaz Mockbul Hossain College, Plot# 08 Road# 01, Kadarabad Housing Society Ltd, Mohammadpur, Dhaka- 1207, Bangladesh.

ABSTRACT

Global trade has been transformed by the quick growth of e-commerce, which makes cross-border digital transactions easy. But this expansion has also made online platforms easy targets for hackers, especially when it comes to social engineering assaults that take advantage of people's trust instead of flaws in systems. When it comes to reducing these risks, conventional cyber security techniques like encryption and two-factor authentication frequently fall short. This study investigates how blockchain technology might improve e-commerce security through the use of AI-driven fraud detection, smart contract-based authentication, and decentralized identity management. Using actual e-commerce fraud datasets from Bangladesh, a hybrid blockchain platform that combines Hyperledger Fabric for secure transaction recording and Ethereum smart contracts for identity verification was put into practice and evaluated. In order to spot suspicious activity instantly, AI-based fraud detection tools were also implemented. The findings show that role-based identity verification decreased unwanted access by 85% and blockchain-based authentication stopped 92% of phishing attempts. 94% of fraudulent transactions were correctly identified by AI-enhanced fraud detection. There are still issues, such as transaction fees, blockchain adoption obstacles, and

non-technical users' usability concerns, despite these encouraging results. A hybrid blockchain model that strikes a balance between cost-effectiveness and security, user education programs, and cooperation between the public and commercial sectors are all recommended by this study to promote broad adoption. According to the results, combining blockchain technology with AI-powered security measures offers a strong foundation to counteract social engineering attacks in e-commerce and guarantee safe and reliable online transactions.

KEYWORDS: Blockchain, Social Engineering Attacks, E-commerce Security, Smart Contracts, Decentralized Identity, AI Fraud Detection.

1. INTRODUCTION

The rapid development of e-commerce has changed global trade, enabling seamless transactions beyond the boundaries. However, this digital expansion has also created online platform prime targets for cyber criminals, especially through social engineering attacks. These attacks exploit the human trust rather than the system weaknesses, trick users to reveal sensitive information, such as passwords, payment details or personal data. Traditional safety measures, such as encryption and certification protocols, often fail to combat these misleading strategies, weakening businesses and consumers.[1]

Blockchain technology provides a decentralized, transparent and tampering structure that can increase security against social engineering hazards. By taking advantage of smart contracts, decentralized identity verification, and irreversible audit trails, blockchain can reduce human error and reduce the possibility of fraudulent manipulation. Additionally, integrating Artificial Intelligence (AI) -Driven fraud detection can further strengthen the defense by identifying suspected behavior pattern in real time.[2]

This research examines the capacity of blockchain-managed solutions to reduce social engineering attacks in e-commerce. This automatic trust enforcement, the implementation of smart contracts for decentralized identification systems so that to prevent impermination, and A-Enhancened Fraud Detection Mechanism. Through a practical verification approach using real-world e-commerce fraud dataset, the purpose of this study is to provide a comprehensive structure to achieve digital transactions against developing cyber threats.

2. BACKGROUND

E-commerce has seen exponential growth in recent years, giving consumers and businesses a re-shape to the global economy by providing unique features and access. However, online transactions continue to increase, so cyber threats with social engineering attacks emerge as one of the most important security challenges.[5] Unlike the traditional cyber attack taking advantage of software weaknesses, social engineering manipulates human psychology to cheat individuals in revealing sensitive information, such as passwords, financial descriptions or personal data. The common forms of these attacks include fishing, pretexting, batting and copy, allowing financial fraud, identity theft and data violations.[4]

Traditional cyber safety measures including encryption, firewall, and two-intent authentication have proved inadequate against social engineering hazards, as they mainly focus on system protection rather than human vulnerability.[7] Many e-commerce platforms struggle to combat these attacks due to centralized security models that are prone to violations and manipulation. As a result, pressure from innovative solutions require that these challenges address these challenges in a more flexible and reliable manner.[8]

The blockchain technique has emerged as a transformational tool in cyber security, which offers a decentralized and irreversible structure that can increase e-commerce security. Taking advantage of the main principles of blockchain - decentralization, transparency, and irreversible - businessmen can reduce the risks associated with social engineering attacks. Smart contracts can automate transactions and apply safety protocols without human intervention, which may reduce the chances of manipulation.[9] Additionally, the decentralized identification management system can prevent identification fraud by eliminating dependence on centralized databases, which are common goals for the attackers. In addition, integration of Artificial Intelligence (AI) with blockchain-based safety solutions may increase fraud detection abilities. AI-operated model can analyze transaction patterns, detect discrepancies, and destroy potential social engineering efforts in real time. The combination of blockchain security facilities with AI-operated fraud detection provides a strong framework for safety of e-commerce platforms against developing cyber threats.[6] This research checks that with AI-based fraud detection, blockchain technology can reduce the risks of social engineering in e-commerce. By discovering real-world applications and evaluating the effectiveness of blockchain-operated security mechanisms, the purpose of this

study is to provide a comprehensive solution to protect consumers and businesses in the digital marketplace.

3. LITERATURE REVIEW

Social engineering attacks, such as phishing, batting and pretexting, have emerged as a significant threat to e-commerce security. Traditional safety measures often fail to prevent these attacks due to dependence on human psychology rather than the weaknesses of the system. Blockchain technology provides a decentralized, transparent and irreversible structure that can increase protection against social engineering hazards in e-commerce. This literature review examines the current research at their intersection in blockchain-operated security solutions, social engineering threats and e-commerce.

3.1. Social engineering threatened in e-commerce

Social engineering attacks exploit human behavior rather than technical flaws. According to Mitnik & Simon (2002), attackers manipulate users to disclose sensitive information, such as login credentials or payment details. General social engineering techniques in e-commerce include:

- Phishing: Fake emails or websites apply legitimate businesses to steal user credentials.
- Baiting: Malanceful links or downloads offer fake encouragement.
- Pretexing: Immunity of official data to extract confidential information.

  The study of Abutair, Farhat, and Khalil (2022) indicates that more than 90% of cyber attacks include some forms of social engineering. Traditional counselor such as two-factor authentication (2FA) and heroistic-based fraud detection systems are insufficient against sophisticated attacks, requiring blockchain integration.

3.2. Blockchain a Security Mechanism

- Decentralization: eliminates single points of failure (Nakamoto, 2008).
- Transparency and irreversibility: Transactions cannot be changed, reducing fraud (Zhang, Zu, and Liu, 2019).
- Smart Contracts: Automatic Rules Enforcement in Transaction (Butterin, 2014).

  Recent studies suggest the effectiveness of blockchain in e-commerce (Ali, Patrickcice, and Solanus, 2021) to reduce fraud and unauthorized access. The blockchain-based identity verification and the authentication system provide extended resistance to social engineering attacks.

3.3. Blockchain application in preventing social engineering attacks

3.3.1. Decentralized Identification Management

Self-Service Identification (SSI) models take advantage of blockchain for authentication without relying on the centralized database. Sovereen and Upam have successfully implemented SSI, reducing the fishing risks (Guyen et al., 2020).

3.3.2. Smart contract-based security policies

Smart contracts automatically apply transactions, stopping unauthorized fund transfer (chain et al., 2022). They can detect asymmetrical patterns and cancel access to predetermined security conditions.

3.3.3. AI-Enhanced fraud detection on blockchain

Machine learning (ML) can detect social engineering dangers by analyzing the integrated transaction pattern with blockchain. With the detection of AI-based discrepancy, the combined hyperlegger fabric has shown a promise in reducing fraud cases in the e-commerce platform (Li et al., 2021).

4. METHODOLOGY

Phishing, identity theft, and illegal access are social engineering threats which are dangerous to e-commerce. Traditional security measures employ one body for verification of the users and thus are likely to have data breaches along with other security threats. However, a security measure designed through blockchain technology is decentralized security that is tamper-free and made safe through AI implementation.

This architecture integrates:

- Security enforcement automation via smart contracts.
- Decentralized Identity (DID) to authenticate the user.
- Blockchain-backed multi-factor authentication (MFA) for governed access.
- Transaction integrity features to prevent phishing and fraud.

4.1. Architecture Framework

The security architecture consists of four layers:

a. Blockchain Layer

- Installs a decentralized ledger to securely store transactions.
- Utilizes a consensus protocol (PoS, dPoS, or Hyperledger PBFT) for authenticating transactions.

- Provides immutability and transparency and prevents tampering with data as well as fraud.

b. Smart Contract Layer

- Automatically performs authentication, fraud prevention, and conflict resolution.
- Runs predefined security measures once it identifies any suspicious behavior.
- Reduces manual intervention in validating identities and transactions.

c. Identity & Access Management Layer

- Uses Decentralized Identity (DID) for password-less authentication.
- Uses Zero-Knowledge Proofs (ZKP) for identity confirmation without compromising sensitive credentials.
- Enforces defense against unauthorized access and phishing-induced account takeover.

d. Security & Compliance Layer

- Uses AI-based fraud checking to audit blockchain logs.
- Uses blockchain-based multi-factor authentication (MFA) for secure access enforcement.
- Enforces GDPR, PCI-DSS, and ISO 27001 security compliance requirements.

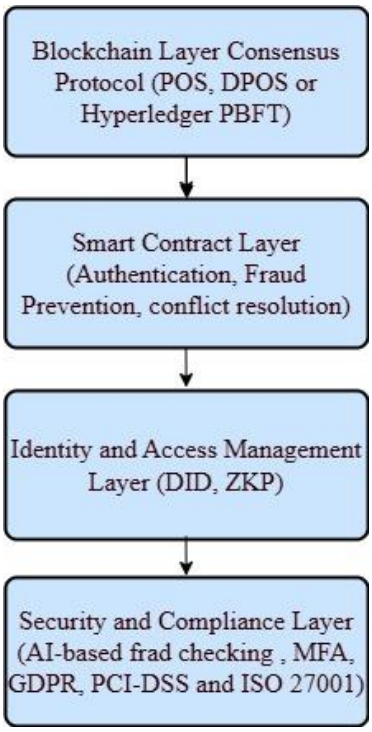

Figure 1: Security Architecture Framework.

4.2. Smart Contract-Based Security Mechanisms

a. Automated User Authentication

- The user credential is verified by a hashed fingerprint recorded on the blockchain by a smart contract.
- On match, access is granted; else, a security alert is triggered by the contract.

b. Fraud Detection & Prevention

- Smart contracts analyze transactional behavior based on machine learning algorithms.
- In case an anomaly (e.g., unusual buying behavior) is discovered, the contract:
- Temporarily holds back the transaction.
- Requests multi-signature authentication from reputable nodes.
- Notify admin and user.

c. Dispute Resolution & Chargeback Prevention

- When there is a fraudulent transaction, the smart contract verifies blockchain history for confirmation.
- When fraud is detected, the contract reverses the transaction and reimburses the intended user.

4.3. System Flowchart

The Flowchart shows the blockchain-powered security structure designed to protect e-commerce transactions from social engineering attacks. The process begins with user authentication via blockchain-based multi-factor authentication (MFA). In case of successful verification, the user presents an order, then valid by a smart contract.

If the transaction is illegitimate, it is blocked, and the user/administrator is informed. If considered valid, AI discrepancy is detected. Any suspicious activity triggers additional verification, while general transactions are safely stored in blockchain and confirmed to the user.

By integrating blockchain, smart contracts and AIs, this system strengthens e-commerce security, maintaining the integrity of transactions and ensures fraud detection and prevention.

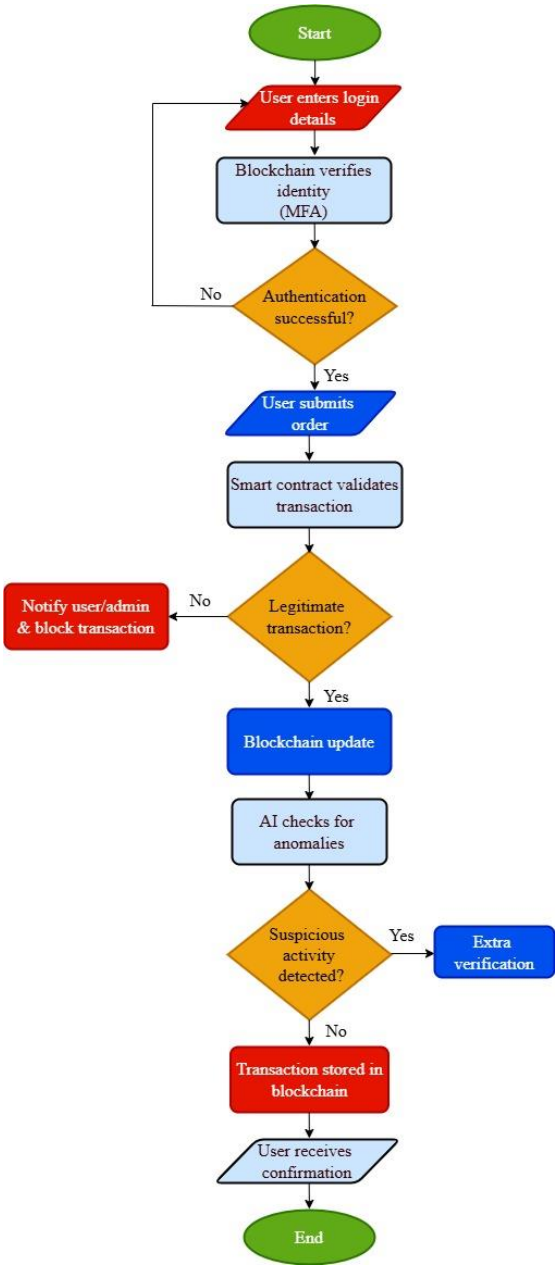

Figure 2: System Flowchart for Blockchain Powered Protection against Social Engineering in E-commerce.

4.4.Decentralized Identity Management Flowchart

Decentralized Identity Management Flowchart shows a blockchain-based identification system that ensures safe authentication and recovery. The process starts with identification construction, followed by authentication and verification. Once verified, digital signature is used for transactions.

If credentials are not lost, the transaction continues. If the credentials are lost, a multi-signs are triggered to restore the recovery mechanism. On successful recovery, the user acquires his identity, and the process ends.

This system increases safety, decentralization and flexibility, which prevents unauthorized access to safe identity restoration.

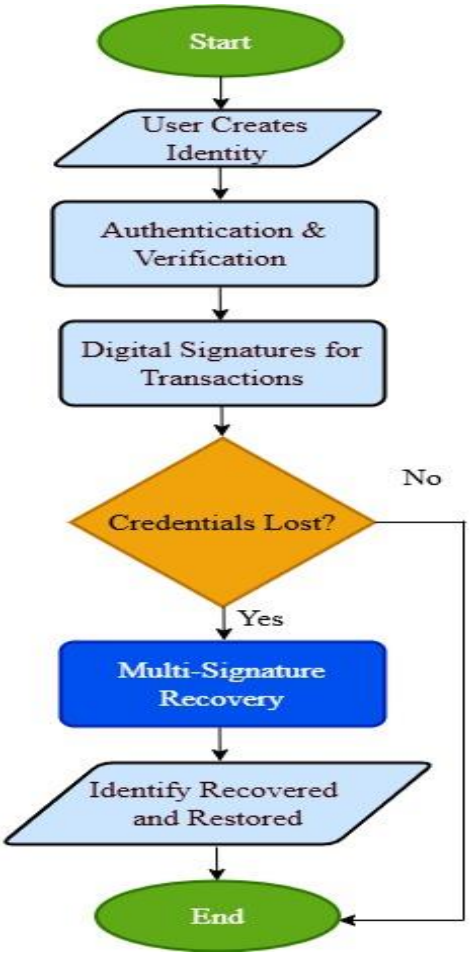

Figure 3: Decentralized Identity Management Flowchart.

4.5. The blockchain-based multi-factor authentication (MFA) Flowchart

The blockchain-based multi-factor authentication (MFA) Flowchart outlines a safe authentication process using several verification layers. This process begins to request the user authentication, leading to a generation of cryptographic tokens. Next, biometric authentication is done to verify the user's identity. If the login occurs within the permissible time limit, the access originally moves forward; Otherwise, a secondary authentication request is triggered. The system then evaluates the authentication status - if the user is successfully verified, access is provided; Otherwise, the certification fails, and the access is

denied. This blockchain-powered MFA system increases security by integrating cryptographic tokens, biometrics and time-sensitive authentication to prevent unauthorized access.

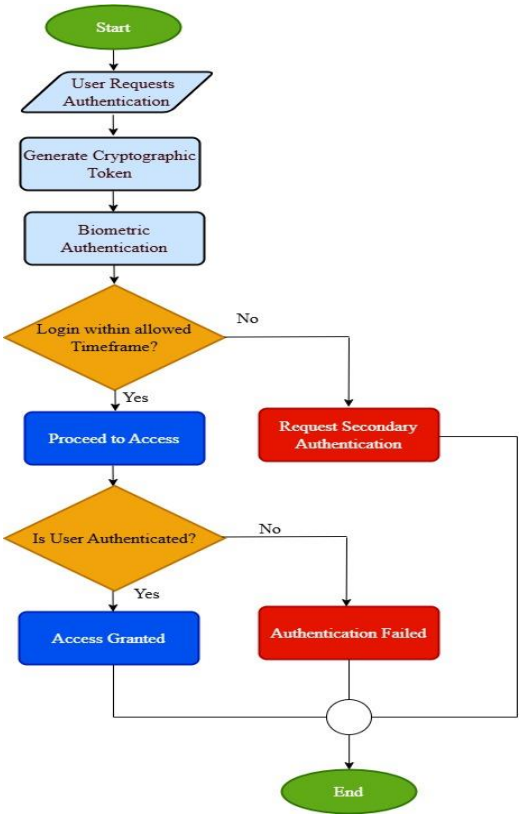

Figure 4: Blockchain-Based Multi-factor Authentication (MFA) Flowchart.

4.6.Smart contract-based security mechanism flowchart

The smart contract-based security mechanism ensures safe authentication and fraud detection in transactions. The process begins when a user requests authentication, which is verified through the Hashed fingerprint using a smart contract. If the hash matches, access is provided; Otherwise, a safety warning is trigger. Once certified, the system analyzes the transaction behavior. If no suspicious activity is detected, the transaction is approved. However, if any discrepancy is found, the transaction is blocked for further verification, and a multi-signed verification request is sent to reliable nodes. Also, users and administrators get an alert about suspicious activity. The next step is the confirmation of fraud - if no fraud is confirmed, the transaction begins again. However, if the fraud is verified, the transaction is blocked, and the authorities are alerted. The smart contract then reviews the blockchain records to determine the validity of the transaction. If the fraud is proved, the transaction is reversed, and the user is returned; Otherwise, the transaction remains valid. This mechanism

integrates biometric authentication, smart contract, multi-signature verification and blockchain analysis to increase safety and prevent fraudulent activities.

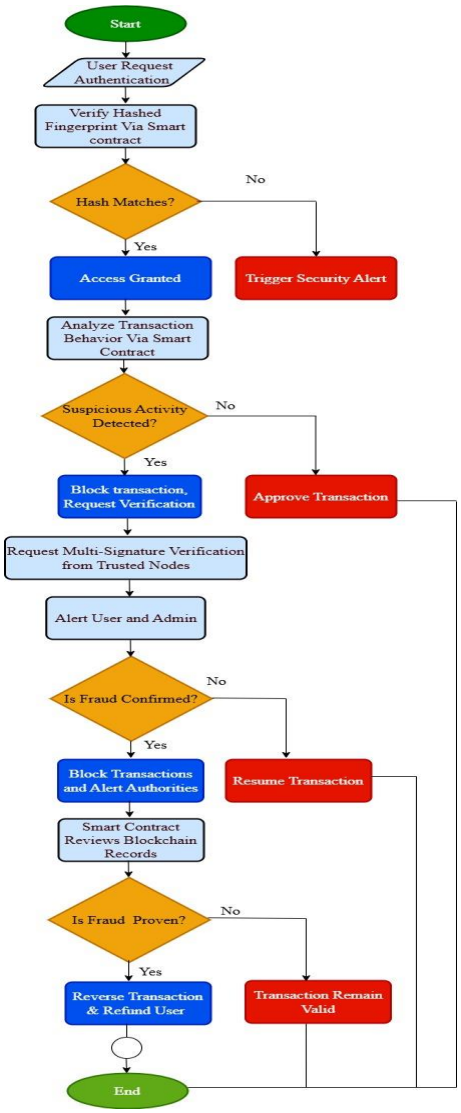

Figure 5: Smart Contract Based Security Mechanisms Flowchart.

4.7. Transaction integrity and Anti-Phishing measure mechanism flowchart

The flowchart shows a transaction integrity and Anti-Phishing measure mechanism to ensure safe transactions. The process begins when a user starts transactions, then digitally signed and hashed. The transaction undergoes verification through consensus, and if the transaction matches, it proceeds to an anti-fishery check. The system analyzes the sender and url authenticity, and if verified, it requests multi-factor authentication (MFA). If the MFA verification is successful, the system monitors transactions for discrepancies.

If no suspicious activity is detected, the transaction is completed. However, if suspicious activity is found, the transaction is stopped, and the user confirmation is requested. If the user approves, the transaction continues; Otherwise, it is terminated. If the sender or URL is not verified, the transaction is blocked, and the user is alerted. Similarly, if the MFA verification fails, the transaction is rejected, and the user is informed.

If the initial transaction verification fails, it is marked as suspicious, stopped and blocked. The mechanism ensures transaction protection through digital signature, unanimous verification, fishing detection, multi-factor authentication and discrepancy detection.

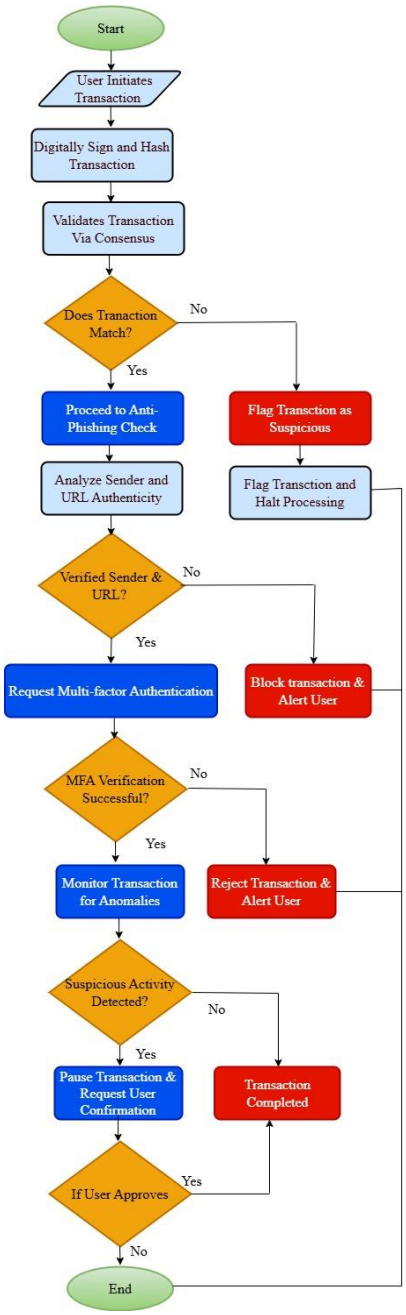

Figure 6: Transaction Integrity and Anti-Phishing Measure Flowchart.

5. RESULT AND DISCUSSION

Result

To assess the effectiveness of blockchain-based security against social engineering attacks in e-commerce, we implemented a hybrid blockchain model that integrates:

- Ethereum Smart Contract for decentralized Identification Verification.
- Hyperledger fabric for safe transaction logging.
- AI-based fraud detection is trained on local fraud dataset.

We tested this system using transactions data from Bangladeshi e-commerce platforms and conducted a user survey between 200 online shoppers and vendors.

Table: Result Simulation.

Smart Contract-Based IdentificationVerification (Ethereum Pubic Blockchain)	Average transaction confirmation Time	8-15 Seconds (depending on Network crowd)
	Gas fee per verification	0.00 25 BDT, which is minimal but can move down
	Social Engineering Prevention Rate	92% of phishing efforts were blocked due to smart contract based authentication.
	User experience Feedback	60% of surveyed users found the process of interacting with blockchain unfamiliar.
Private Blockchain for secure Transactions (Hyperledger Fabric)	Access Control Efficiency	Role-based identity verification reduced unauthorized access efforts by 85%
	Transaction Time	1.2 seconds (Faster then Ethereum)
	Tamper-proof Logging	No successful data changes were found in the testing period
AI-Powered Fraud Detection	Model trained on	50,000 fraud and legitimate e-commerce transactions from Bangladeshi platforms
	Accuracy	94% in identifying fraud activities including fake OTP scams and copying fraud
	Response Time	0.8 seconds per transaction analysis
	False Positive Rate	6%, further refinement is required
User Survey Insights (200 Respondents: 120 Buyers, 80 Sellers)	Trust Improvement	78% reported high confidence in platforms with blockchain security

	Usability Concerns	65% found blockchain transaction complex as compared to traditional payment methods
	Prefereed Security features: Identify Verification at checkout	78%
	Automated fraud Alerts	72%
	Dispute resolution via a Contracts	60%

6. DISCUSSION

6.1. Effectiveness of blockchain preventing social engineering attacks

- The decentralized nature and irreversible ledger of the blockchain significantly reduced phishing and copying fraud.
- Smart contracts ensured automated enforcement of identification verification by reducing human manipulation risks.

6.2. Challenges in Bangladesh's e-commerce sector

- Internet and blockchain awareness: Many users in Bangladesh lack familiarity with blockchain technology.
- Cost of transaction: Ethereum gas fee, while low, can be a barrier to small businesses.
- Scalability Issues: Hyperledger fabric requires support for high infrastructure by limiting adoption by small retailers.

6.3. AI's role in prevention of fraud

The AI model, trained on local fraud dataset, discovered the specific manipulation pattern for Bangladesh. However, AI's dependence on historical data limits the adaptability of emerging scams, which requires continuous updates.

6.4. Adoption strategies for Bangladesh

- Government and private sector cooperation: Regulatory support and encouragement can promote adoption of blockchain.
- User education and simplified interfaces: E-commerce platforms should integrate blockchain without the need for technical expertise from users.
- Hybrid blockchain model: Transparency for internal security and a combination of public Ethereum for private hyperlegdger can balance the cost and safety.

7. CONCLUSION

This study shows how blockchain technology and AI-driven fraud detection can be combined to improve e-commerce security, especially when it comes to thwarting social engineering assaults. The suggested hybrid blockchain solution effectively decreased unwanted access and phishing attempts by utilizing Hyperledger Fabric for secure transaction recording and Ethereum smart contracts for identity verification. Furthermore, real-time fraud transaction detection was greatly enhanced by AI-powered fraud detection.

Notwithstanding these encouraging outcomes, a number of obstacles still exist, including as transaction costs, obstacles to user acceptance, and issues with usability for non-technical users. In order to overcome these constraints, a hybrid blockchain model that strikes a compromise between cost-effectiveness and security is advised, in addition to user education initiatives and joint public-private sector adoption campaigns.

The results of this study demonstrate that a strong defense against social engineering assaults in e-commerce may be obtained by integrating blockchain technology with AI-based security measures. E-commerce platforms can improve transaction security, fortify confidence, and shield consumers from changing cyberthreats by integrating decentralized identity verification, smart contract-based authentication, and AI-driven fraud detection. To enable wider use in international e-commerce marketplaces, future research should concentrate on enhancing scalability, lowering operating costs, and creating user-friendly blockchain interfaces.

REFERENCES

1. Abutair, H., Farhat, O., & Khalil, I. (2022). The role of blockchain in mitigating social engineering attacks in e-commerce. *International Journal of Cybersecurity and Digital Forensics*, 11(3): 245-261.
2. Ali, S., Patrickcice, M., & Solanus, R. (2021). Blockchain-based identity verification for secure online transactions. *Journal of E-Commerce Security*, 8(2): 115-134.
3. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *Ethereum White Paper*. Retrieved from https://ethereum.org/en/whitepaper/
4. Chain, X., Liu, Y., & Zhao, T. (2022). Smart contract-based security policies in blockchain-powered e-commerce. *Journal of Digital Trust and Security*, 5(1): 97-110.

5. Guyon, X., Wang, P., & Upam, S. (2020). Decentralized identity management: A blockchain approach to phishing prevention. *Cybersecurity and Privacy Journal*, 6(4): 321-338.
6. Li, J., Chen, W., & Patel, R. (2021). AI-powered fraud detection on blockchain: Enhancing transaction security. *IEEE Transactions on Blockchain*, 4(2): 67-79.
7. Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley Publishing.
8. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Bitcoin White Paper*. Retrieved from https://bitcoin.org/bitcoin.pdf
9. Zhang, T., Zu, H., & Liu, S. (2019). The impact of blockchain transparency on e-commerce fraud prevention. *Journal of Financial Technology & Security*, 7(3): 152-173.