WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Data Privacy and Security in E-Commerce

Mr. Prakash Hongal[1] , Dr. Aruna Kumar Joshi[2], Ms. Preeti Katti[3]

[1,2,3]Department of CSE, Smt Kamala and Shri Venkappa M Agadi College of Engineering and Technology Lakshmeshwar, Gadag 582101, India

A B S T R A C T

In the developing ecommerce landscape, data protection and security have become paramount, thanks to the increased number of cyber threats and sophisticated attacks. This summary examines the integration of blockchain technology and multifactorial authentication (MFA) as a complementary solution to improve transaction security and ensure data integrity to ecommerce platform. A decentralized and immutable ledger technology, Blockchain provides a robust framework for protecting ecommerce transactions by providing transparency and traceability. All transactions are recorded in encrypted, secure blocks and added to the chain of previous transactions. This unique feature of blockchain technology significantly reduces the risk of fraud and unauthorized data manipulation to ensure that transaction records remain accurate and reliable. Multifactor Authentication (MFA) on the other hand adds additional levels of security through several types of reviews before accessing sensitive information or transactional degrees.

Keywords: Block chain, Multi-Factor Authentication, E-commerce, Data Privacy, Transaction Security, Data Integrity, Cyber security, Fraud Prevention, Authentication Methods.

1. Introduction

The rise of e-commerce has changed the global market. This allows for seamless transactions and increases consumer comfort. However, this high-speed digital expansion has raised major concerns about data protection and security in the data protection area. Online platforms process huge amounts of sensitive information, including personal data, payment details, transaction stories and more. This means that it is presented for cyberattacks such as data injury, identity theft, or financial fraud. The security of these transactions is important to maintain consumer trust and maintain the integrity of digital trade.

In recent years, blockchain technology and multifactor authentication (MFA) have proven to be promising solutions to improve security measurement in ecommerce environments. The decentralized architecture of blockchain provides transparency, immutability and resistance to manipulation. This makes it extremely effective when protecting transactional data. By distributing data over a network of nodes, blockchain reduces the risk of individual point errors and unauthorized access, leaving transaction records safe and verifiable. Traditional authentication methods such as passwords are susceptible to brute force attacks, phishing, and login information. MFA reduces these risks through a combination of factors such as adhesives, biometry, single passcodes, and device based authentication, as it greatly enhances access control mechanisms. By examining the effectiveness of the combination, this study aims to demonstrate how these technologies address existing weaknesses, improve data protection and create a more resistant digital ecosystem.

To address these challenges, there is an urgent need for a robust safety frame that protects sensitive data and ensures transaction integrity. Blockchain technology and Multifactorial Authentication (MFA) are being developed as promising solutions that can enhance ecommerce security. Transactional data is stored in main registers distributed across several nodes, making it naturally manipulated by the decentralized and invariant nature of the blockchain. All transactions are encrypted to previous transactions to create a transparent, secure record that improves trust and reduces the risk of fraud.

This multilayer approach significantly reduces the chances of unauthorized access, even if authentication coefficients are affected. Blockchain ensures data immutability and decentralization, while MFA increases user authentication and together creates robust defences against ecommerce cyber threats.

This paper deals with the use of these technologies in a combination, examining the potential for a more secure environment for redefine data security practices and online transactions.

2. Literature survey:

Increasing digitalization of trade has posed important challenges in relation to data protection and security. Researchers have considered numerous strategies to reduce these risks, and blockchain and multifactorial authentication (MFA) are promising technologies to protect transactions. This section checks out important research and technological advances that have contributed to strengthening e-commerce security.

2.1 Block chain Technology in E-commerce Security:

Blockchain technology is largely considered in its ability to improve the transparency, integrity and security of digital transactions. Nakamoto (2008) first introduced blockchain as a decentralized main book technology to secure Bit coin transactions, demonstrating the possibility of eliminating central failures and preventing non-exempt data manipulation. Since then, researchers have been investigating a wide range of applications in e-commerce.

Zhang et al. (2019) highlighted the role of blockchain in ensuring transactional transparency due to its decentralized nature. Her research showed that all transactions were encrypted connected to the previous transaction, making data almost impossible. Additionally, intelligent contract agreements with predefined rules automation in the e-commerce process were investigated. This reduces the need for security and intermediaries.

In a similar way, Ramezani an et al. (2020) proposed a blockchain-based identity testing system to protect user identity and financial data during e-commerce transactions. Your research shows that blockchain not only improves data integrity, but also takes into account data protection concerns by using users to control access to personal data.

2.2 Multifactor authentication for access control:

MFA has been developed as a robust security measure aimed at reducing unauthorized access through layered authentication mechanisms. Bonneau et al (

2015) examined the weaknesses of traditional password based systems and recommended MFA as a solution to enhance user authentication.

By combining several validation factors such as passwords, biometry and OTP, MFA increases the complexity of the authentication process, making it

much more difficult for attackers to circumvent safety measures. Their results showed that the implementation of MFA did not reduce 70% access to access, increasing the importance of implementing a multilayer authentication mechanism.

alotaibi et al. (2022) further explored biometric integration as part of MFA. Her research showed that the use of biometrics such as fingerprints and facial recognition not only improves security, but also improves user experience through the filling of the authentication process.

The need for a robust user authentication method has controlled the deployment of MFA across digital platforms. et al. (2017) examined the effectiveness of MFA to reduce unauthorized access to ecommerce environments. Her study showed that several authentication factors, such as passwords, biometrics and device-based validation, were reduced by 85%, not authorized attempts to register.

acar et al. (2018) analysed user friendly and safe waste when accepting MFA. The study also highlighted that while users recognized that multistep authentication was slightly impractical, additional security groups also effectively countered phishing attacks and login information. Biometric integration used research to streamline the user experience and maintain standards at the same time with a high level of security.

2.3 Integration of Blockchain and Multifactor Authentication:

The current study examined the synergistic effects of blockchain and MFA during the creation of robust safety frames. Xu et al. (2020) proposed a blockchain based identity testing system integrated with MFA to protect user accounts and transactions.

Another study by Kumar et al. (2021) introduced a hybrid model that uses blockchain to manage digital identity, and MFA added an additional layer of security. The results showed a 60% reduction in unauthorized attempts to access and a 50% increase in transaction transparency

The combination of blockchain and MFA has recently highlighted the possibility of creating a comprehensive security framework. Li et al. (2022) proposed a hybrid model that integrates blockchain for transaction recording and integrates MFA for access control. Her research showed that this double-variation approach significantly reduces the risk of unauthorized access and fraudulent behaviour in e-commerce systems.

In addition, Singh et al. (2023) examined the use of blockchain when managing authentication data. Her research suggested storing hash authentication registration information on the blockchain to ensure that sensitive data is still secure even if the system is affected. This study highlighted that blockchain integration in MFA provides an additional layer of protection and that e-commerce platforms are resistant to developing cyber threats.

2.4 Challenges and Future Directions:

Blockchain and MFA present promising security improvements, but researchers have identified several challenges. For example, Lin and Liao (2017) highlighted the issue of blockchain scalability. This issue can increase transaction review times with strong network loads. Similarly, the MFA system is Krol et al. It is often exposed to user resistance due to additional complexity such as. (2019).

Future research like Patel et al. (2023) suggests implementing a light blockchain framework specifically developed for ecommerce, reducing transaction time and improving scalability. Furthermore, the integration of artificial intelligence (AI) will develop to recognize suspicious activities and adapt MFA requirements in real time as promising research roads.

3. Application

The integration of blockchain and multifactor authentication (MFA) in ecommerce has made significant advances in protecting digital transactions and protecting user data. These technologies are used in many aspects of ecommerce to improve security, transparency and trust. Some important applications include:

3.1 Secure Payment Processing:

Blockchain technology is widely used in protecting payment transactions. Traditional payment methods are often based on centralized systems, making them more susceptible to data injuries and fraud. Blockchain eliminates these risks for decentralized transactional documents and ensures that each payment is checked by the node's network before an unchangeable lid is added. This increases transparency and prevents double expenses or unauthorized changes. Integrating MFA adds another level of security that allows users to verify their identity by several factors before processing payments, reducing the risk of unauthorized transactions.

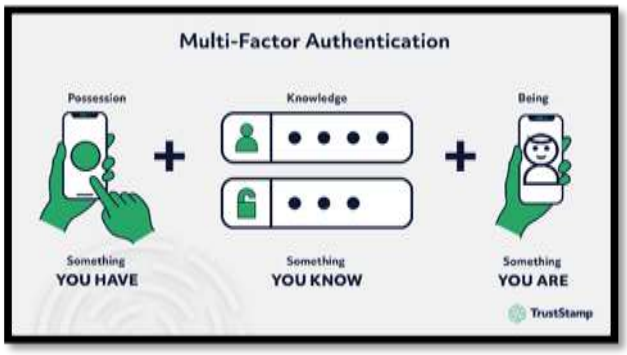

Fig. 1 –MFA

3.2 Identity inspection and access control:

Identity inspection and access control are critical components of cybersecurity, ensuring that only authorized users and devices can access systems and data. Identity inspection involves verifying user credentials, behaviour, and attributes to detect anomalies or potential threats. Access control enforces policies that define who can access what resources, using methods like role-based access control (RBAC), multi-factor authentication (MFA), and least privilege principles. Together, these mechanisms enhance security by preventing unauthorized access and mitigating risks associated with data breaches and insider threats.

3.3. Preventing fraud and integrity of transactions

Blockchain immutability makes fraudulent activities extremely difficult as transactions cannot be changed or deleted. All transactions are encrypted and connected to previous transactions. This provides a transparent test route that allows you to verify the validity of each transaction. MFA adds additional protection by allowing only validated users to start or approve the transaction. This means that the risk of fraud can be further minimized.

Fig. 2 – Fraud Detection

3.4 Supply of Transparency:

E-commerce companies use blockchain to improve supply chain transparency. By recording every step of the supply chain in a distributed general book, companies can pursue product origins, shipping status and delivery time planning in real time. MFA integration allows only certified employees to update or access delivered data that protects information integrity and prevents unauthorized operations.

Fig. 3 – Block chain

3.5 Data Protection and Data Protection Compliance:

With growing concerns about data protection and regulations such as the GDPR and CCPA, ecommerce companies occupy blockchain to protect user data. Blockchain provides a secure way to store and share personal data that is only accessible via encryption keys. MFA further strengthen this system by ensuring access requirements are subject to a strict authentication process. This protects your personal data from unauthorized access and cyberattacks.

Fig. 4 - Data Protection and Data Protection Compliance

3.6 Loyalty Programs and Reward Systems:

Blockchain is increasingly being used to manage ecommerce loyalty programs. Traditional loyalty systems often suffer from fraud and lack of transparency. Using blockchain, businesses can create a transparent reward system where points and transactions are recorded in a decentralized main

register. MFA guarantees that only real users can claim rewards. This improves unauthorized access to loyalty accounts and increases trust between customers and businesses

Fig. 5 - Loyalty Programs and Reward Systems

3.7 Dispute resolution and feedback:

Disputes relating to transactions and feedback are common in ecommerce. Blockchain transparent transaction records simplify resolution by providing an immutable transaction history. The MFA adds another level of security by allowing only approved persons to initiate refunds or dispute inquiries. This prevents unauthorized withdrawal.

3.8 Smart Contracts for Secure Transactions:

Block chain based smart contracts automatically execute transactions when predefined condition are met, reducing the need for intermediaries.

For example, you can only release payments if the product is confirmed to be delivered. MFA adds another level of security so that only authenticated parties can trigger the execution of these contracts and therefore minimize unauthorized transactions.

Conclusion

In the rapidly evolving ecommerce situation, robust data protection and security assurances are extremely important for building trust and protecting digital transactions. In this article, we examined the integration of blockchain and multifactorial authentication (MFA) as a complementary technology to address these challenges. The decentralized and immutable nature of blockchain provides unprecedented data integrity by recording distributed nodes securely, minimizing the risk of unauthorized changes and fraud. At the same time, MFAs will enhance access control by requiring several review factors and significantly reducing the likelihood of unauthorized access, identity theft and password related weaknesses.

Blockchain ensures that transaction records continue to be manipulated, and MFA strengthens authentication mechanisms, making it more exponentiall y difficult for malicious actors to exploit security gaps. This synergistic approach provides a comprehensive solution to growing concerns about ecomm ere injuries and cyberattacks. Future research can explore the integration of new technologies such as Artificial Intelligence (KI) and Zero Trust Archite cture (ZTA) to optimize blockchain scalability, improve MFA ease of use, and further enhance safety frameworks. Ultimately, blockchain and MFA int egratin not only enhances user data protection, but also paves the way for a more secure, transparent and resilient digital market.

References

[1] Yanamara, Anil Kumar Yadav. "Sensitive deep learning for hospital predictions Elimination: Improved patient care and resource allocation." International Journal of Advanced Engineering Technologies and Innovations 1.3 (2022): 56-81. [2] Suryadevara, Srikanth, Anil Kumar Yadav Yanamala. "Patients Use Artificial Intelligence in Health Care." International Journal of Machine Learning Cybersecurity and Artificial Intelligence Research 11.1 (2020): 30-48.

[3] Suryadevara, Srikanth. "Optimizing Wireless Hart's Real-Time Task Planning Network: Challenges and Solutions." International Journal of Advanced Engineering Technologies and Innovations 1.3 (2022): 29-55.

[4] X. Liu, Y. Zhang, and L. Wang – "Block chain-Based Multi-Factor Authentication Framework for Secure E-Commerce Transactions" – Focuses on combining block chain and MFA to enhance user identity verification and secure online transactions.

[5] R. Singh and P. Kumar – "A Block chain and Multi-Factor Authentication-Based Secure Payment Framework for E-Commerce" – Introduces a hybrid model combining block chain with MFA to prevent unauthorized transactions.

[6] A. Alzahrani and J. Bulusu – "Block chain-Based Privacy-Preserving Authentication Framework for E-Commerce" – Proposes a secure architecture combining block chain with MFA to ensure privacy in e-commerce systems.

[7] H. Kim and M. Lee – "Decentralized Multi-Factor Authentication for E-Commerce Transactions Using Block chain" – Discusses implementing decentralized identity management combined with MFA to improve transaction security.

[8] M. Conti, S. Kumar, C. Lal, and S. Ruj – "A Survey on Security and Privacy Issues of Block chain Technology" – Explores how block chain and MFA can strengthen data protection in e-commerce platforms.

[9] Isakov, Abrah, Faklizinurozov, Shahboz Abduzhappolov, Mukhrisaysokova. "Improved Cybersecurity: Protecting Data in the Digital Age." Science Innovation and Technologies 1, No. 1 (2024): 40-49.

[10] Suryadevara, Srikanth. "Enhancing Brain-Computer Interface Applications through IoT Optimization." Revista de Inteligencia Artificial en Medicina 13.1 (2022): 52-76.