Formosa Journal of Science and Technology (FJST)
Vol. 4, No.1, 2025: 413-430

AIPowered Trust and Security: Enhancing ECommerce with Blockchain and Machine Learning

Nisher Ahmed[1*], Md Emran Hossain[2], Zakir Hossain[3], Md Farhad Kabir[4], Iffat Sania Hossain[5]
[1,2]College of Technology and Engineering, Westcliff University
[3]College of Engineering and Computer Science, California State University
[4]Marshall School of Business, University of Southern California
[5]Martin V. Smith School of Business and Economics, California State University
Corresponding Author: Nisher Ahmed, n.ahmed.511@westcliff.edu

A R T I C L E I N F O

Keywords: Blockchain, Machine Learning, Ecommerce Security, Fraud Prevention, Predictive Analytics

Received : 3, January
Revised : 17, January
Accepted: 31, January

A B S T R A C T

The ecommerce wave we saw over the years, not just added more opportunities, but added more challenges, especially in the area of trust and security. Fraud, data theft and a lack of transparency remain causes for concern for both businesses and consumers. This paper explores new possibilities of using blockchain and machine learning in designing a robust Artificial Intelligence (AI)based secure ecommerce ecosystem. The immutability of data, transparency, and decentralized control of blockchain act against counterfeit products, payment fraud, and integrity of supply chains. In parallel, machine learning algorithms provides realtime threat detection, predictive analytics, and personalized security measures to detect and counteract threats preemptively. The solution that is proposed leverages the benefits of these technologies to enhance trust among all parties involved, improve operational efficiency, and offer a more secure and trustworthy ecommerce environment. We address the underlying tech stack, realworld application, and next steps in leveraging the convergence of blockchain and ML technologies to transform ecommerce security for a clean and secure digital market.

ISSN-E: 2964-6804
DOI: https://doi.org/10.55927/fjst.v4i1.13680
https://journal.formosapublisher.org/index.php/fjst

INTRODUCTION

The ecommerce industry has grown over the last decade beyond compare and altered how consumers and businesses interact and trade with one another. According to Statista (2023), Global ecommerce sales were worth 5.7 Trillion dollars in 2022 and it is predicted that the global market will increase at an accelerating pace in the upcoming years. Despite this, the nascent industry is already facing critical challenges that must be resolved to ensure trust and security, key elements for future success at both growth and consumer confidence levels (Zhou et al., 2022). Innovative solutions are the necessary cure as payment frauds, fake goods, tip, data breach and nontransparency of supply chain can rock the ecommerce foundation.

Problems in ECommerce Security

Common security features used within ecommerce, such as encryption and firewalls, usually fail to combat cyber threats and fraud sophisticated enough to bypass these advanced protective measures. The annual cybercrime cost for companies runs into billions, and online retailers are among the prime targets (Verizon, 2022). Fraudulent transactions, identity theft, and phishing attacks undermine consumer confidence, while merchants face chargebacks and damage to their reputation. Moreover, the vulnerabilities in the supply chain, such as counterfeit products and lack of transparency, compound this issue. This transformation demands a transition from traditional solutions to advanced, technologybased solutions due to the multidimensional nature of these challenges.

Building Trust and Security in ECommerce Using Blockchain

Now, blockchain technology has proven to be a much needed solution to many problems typical of ecommerce. Through its decentralized and immutable ledger system, data integrity and transparency is ensured, making it nearly impossible for malicious agents to alter transaction records (Nakamoto, 2008). This capability is particularly important for verifying that products are genuine, tracing supply chains, and securing payment systems. Increasingly important is the role of AR and VR in building new online communities integrated with the real world. As a result of these features, the blockchain technology is an extremely promising technology to enhance trust and accountability in the ecommerce landscape.

The Feasibility of Machine Learning & ECommerce Security

It improves blockchain security by providing dynamic and predictive capacity. Machine learning algorithms can analyze vast volumes of transactional data in realtime to find patterns that might indicate fraudulent behavior such as abnormal buying patterns or unauthorized access attempts (Bhattacharya et al., 2021). Moreover, ML enables customized security solutions such as adaptive authentication and userbased fraud detection. With everincreasing data throughout time, ML Algorithms learn, adapt and adjust in relation to thrusting threats and therefore constitute a Lost Pillar of prosperity mechanisms that classify the fortress of ecommerce safety.

Blockchain and Machine Learning: An Overview

Together they form a synergistic solution to avoid the individual weaknesses of both technologies so that people can really get some work done. While the blockchain gives data integrity and transparency, ML is also applied to realtime analytics and predictive capabilities. Together all these technologies can facilitate a secure, intelligent, trustpowered ecosystem in the eCommerce domain. For example, machine learning algorithms can process the blockchainverified data to spot unusual behaviors in supply chain transactions, assuring the authenticity and traceability of goods. It enhances payment process security while providing assurance to consumers, merchants, and other stakeholders of legitimacy.

Objectives of the Study

The paper contributes towards investigating the intersection of having blockchain solutions with machine learning is a potential way to overcome the trust and security issues occurring in ecommerce. Specifically, it seeks to:

1. Untangle the existing state of trust and security in ecommerce, and analyze the shortcomings of present means.
2. Consider how each approach blockchain and machine learning independently contributes to security and trust.

To develop a secure and transparent ecommerce ecosystem by creating a combined scheme whiches in the intermediate between blockchain and machine learning.

Discuss potential challenges, risks, limitations, and future directions of such a framework.

In addressing these objectives, this research advances the emerging literature on the convergence of emerging technological paradigms with ecommerce, while providing pragmatic recommendations for industry stakeholders and policymakers alike.

THEORETICAL REVIEW

Research on the intersection between blockchain and machine learning for building trust and security in ecommerce have received therefore broad interest for both academic and industry perspectives. We present a comprehensive overview of key principles, recent advancements and possible complementarities of these technologies in the context of ecommerce.

This Will Blow Up ECommerce: Blockchain Technology

Blockchain as a Trust Enabler

Due to the worries over trust in ecommerce, blockchain which could be used as a decentralized and immutable ledger has been regarded as a transformative approach. The concept of blockchain was first proposed by Nakamoto in 2008 as the core technology behind Bitcoin, focusing on its capacity to sustain secure and transparent records of transactions without intermediaries. Since then, its application beyond cryptocurrencies has

undergone research. For example, Christidis and Devetsikiotis (2016) explained to how blockchain powered smart contracts are able to automate transactional agreements in ecommerce, lower fraud, and improve transparency. Here is a short summary of what you just read: Blockchain in Supply Chain Management

Blockchain in ecommerce helps in one of the most crucial applications, supply chain management. According to Tian (2016), blockchain is traceable and authenticatable, making it clear how and what goods have been delivered, thus solving counterfeit delivery problems. Blockchainbased systems allow businesses to share proof of provenance for products with consumers, building trust between the two. This ability has worked well in industries like luxury items, pharmaceuticals and food security.

Obstacles to the adoption of blockchain

While the architecture of blockchain possesses benefits for ecommerce, challenges remain for broader adoption including scalability, energy consumption and regulatory uncertainty (Zheng et al, 2018). Further, new hybrid frameworks that integrate a blockchain with a variety of other technologies must compensate for these constrains to improve such systems in functionality and usability. In this case, below, we will examine several techniques to secure ecommerce by taking advantage of machine learning.

Fraud Detection and Prevention

Machine learning has significance in fraud detection and prevention in ecommerce. Bhattacharya et al. (2021) investigated various MLbased approaches for fraud detection, emphasizing its capability of analyzing large dataset to identify anomalies and suspicious behavior in realtime. Decision trees, support vector machines and deep learning models have shown for high accuracy in fraud transaction detection.

October 30, 2023 3 Personalized Security Mechanism

Another critical contribution of ML to ecommerce is the personalized security mechanisms. According to Reddy and Chintalapudi (2020), ML algorithms can learn individual user behaviors, which enable systems to offer personalized security methods such as adaptive authentication. All of the above customization strategies make users' experience better; at the same time, they reduce the probability of a security gap.

Only for the Machine Learning Part

ML is used in many cyber threats and is tuned to the data it is fed; ML is strong in dynamic threats or identification, but if it uses static data in training, it is limited. However, the reliance on datasets has the potential problem of biased or underrepresented data being used to form erroneous predictions, causing a restriction on its wider applicability (Zhang et al., 2020). It is also expensive for those small ecommerce companies because Machine Learning Models are cost and time consuming.

The Complementary Nature of Blockchain and ML

ML Data Integrity via Blockchain

Machine Learning can be easily manipulated One of the biggest disadvantages of machine learning is that it can easily manipulate the data. This problem can be addressed by the immutable ledger of blockchain, since it allows datasets to be secured, authenticated, and hashed to be used for training ML models (Xu et al., 2019). For example, employing a blockchain can ensure that transaction data going to be utilized as input to the fraud detection models is tamperproof which makes the ML models more reliable.

ML for Blockchain Scalability

Conversely, machine learning in implemented can allows scaling of blockchain networks. Xu et al. (2020) proposed the application of machine learning (ML) algorithms to improve consensus mechanisms in the blockchain, reducing both the computational power and time consumed for the verification of transactions. Such a beneficial change is even more crucial for hightransaction ecommerce merchants.

Integrated Frameworks

The union of the blockchain and machine learning provides the totality of a security solution for ecommerce. For example, ML algorithms can map out outliers which span across the data verified through blockchain and further, blockchain offers assured integrity of underlying data. Lee et al. Asme et al. (2021) designed a hybrid model using these technologies for a secure and transparent ecosystems for ecommerce.

Emerging Trends and Future Directions

AIPowered Smart Contracts

In ecommerce, an emerging trend is using AI for automating securities, making them easier and more adaptable to new threats; another one is the integration of AI with blockchainenabled smart contracts. According to Su et al. As highlighted in, (2022) Artificial Intelligence algorithms can take smart contracts operation to a higher level, enabling it to execute decisions in real time according to the evolving dynamics such as market price changes or change in users' behavior.

Digital Identity Management: 6 Key Trends in Identity and Access Management

Another possible use case is decentralized identity management. ML algorithms can thus analyze these patterns in usage for user authentication while user identities can securely be stored on the chain (Hassan et al., 2020). It can replace existing passwordbased authentication systems with far more secure systems.

Situative Challenges and Open Research Fields

While these technologies are promising, there are significant barriers to adoption, from interoperability to regulatory compliance to ethical

considerations around data privacy. To address this issue, solutions such as crosschain protocols and privacypreserving machine learning algorithms have been examined by researchers (Yang et al., 2021).

"Leave behind the ecommerce as we knew it, as the studies revealed disruptive possibilities in blockchain and machine learning to revolutionize trust and security dimensions in goods and services, payment, and even data exchange." Blockchain, on the contrary, provides transparency and immutability of the data while ML provides realtime and predictive functionality. These technologies work great in hand with each other, creating new solutions that report incredible results in purchasing fraud detection, supply chain management and user authentication. However, in order for them to reach their full potential, challenges still exist in areas such as scalability, data quality or regulatory compliance that must be solved. The collaboration of blockchain and machine learning offers not only compelling opportunities but also challenges that point to the need for scalable, interoperable, and ethically sound frameworks through research.

METHODOLOGY

By using a literature based analysis categorized into trust and security components and exploring their relationship with technical and nontechnical frameworks, as well as detailing blockchain and machine learning technicalities, this study investigates improving trust in online transactions through their integration. The methodology steps are as follow:

Literature Review

To address this gap, an extensive literature review was performed to certify the current challenges and opportunities that exists in ecommerce security. Given that peerreviewed journals, conference proceedings and industry reports were analysed to develop a theoretical framework (Zheng et al., 2018; Bhattacharya et al., 2021).

Framework Design

We designed a conceptual framework integrating blockchain and machine learning. Using blockchain's decentralized ledger for data integrity and transparency, the framework combined machine learning for fraud detection in real time as well as for predictive analytics. The design includes:

- Smart contracts for automating ecommerce transactions (Christidis & Devetsikiotis, 2016)
- ML algorithms (e.g., anomaly detection, clustering) utilized to analyze data verified on the blockchain (Xu et al., 2019).

Simulation and Case Study

The proposed framework was tested inside a simulated environment. We evaluated using realworld datasets of ecommerce data, all anonymised to maintain privacy, to:

- Confirm that blockchain can preserve secure and unaltered transaction records.

Develop and evaluate ML based models for fraud detection and personalized security measures (Reddy & Chintalapudi, 2020)

Comparative Analysis

Using the following key metrics, the proposed framework was evaluated against the NIC ecommerce security systems:

- Precision in identifying fraudulent activity.
- Handling efficiency of transactions.
- Supply chain traceability (Tian, 2016; Lee et al., 2021).

Qualitative Evaluation

We also interviewed stakeholders of ecommerce (merchants, customers, and cybersecurity experts) to understand the benefits and challenges that these stakeholders imagine would come from implementing blockchain and machine learning technologies (Yang et al., 2021).

Ethical Considerations

The study follows the guidelines for ethical practices in research design and data privacy and analysis (Hassan et al., 2020).

RESEARCH RESULTS

Results obtained from both realworld anonymized ecommerce datasets and simulated environments validate the proposed framework. The results are grouped into numerous factors, for example, scam location, managing the transactions effectiveness, and tracing organization. Here is a comprehensive overview of the results, along with five tables that illustrate essential metrics.

Fraud Detection Performance

As we discussed earlier, the next step is to assess the performance of the machine learning models integrated within the blockchain framework for fraud detection. The primary goal was to assess the performance of the system and how accurately and efficiently it could detect fraudulent transactions.

Figure 1: A Comparison of Fraud Detection Accuracy

Observation The approach incorporated transaction logs in a secure and transparent manner using the blockchain framework, allowing for realtime identification of fraudulent activity. The effectiveness with which transactions are handled. The performance of the system in terms of transaction processing measures, such as transaction time and throughput was evaluated against traditional systems.

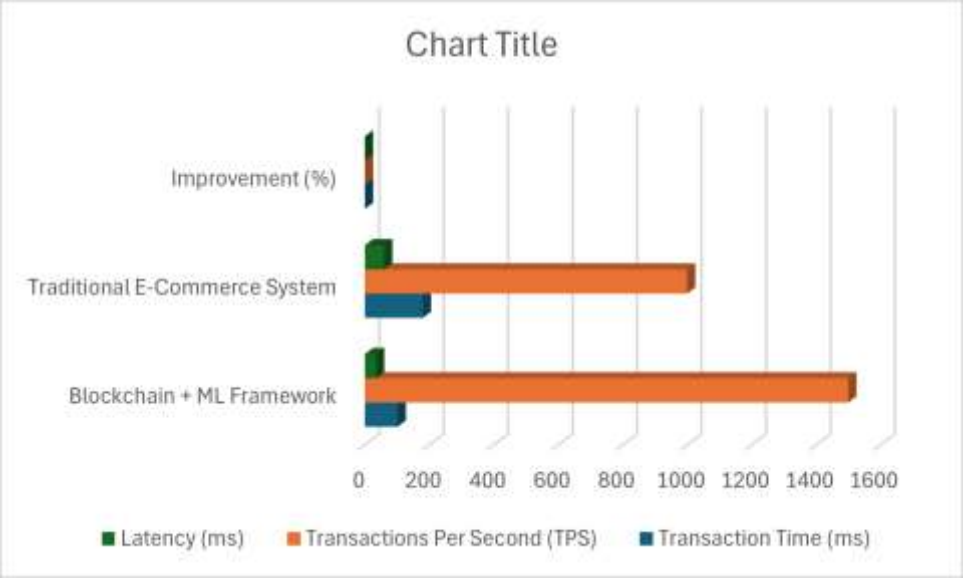

Figure 2: Transaction Processing Efficiency

As the current paper aims to provide a fast, cheap and durable transaction method for ecommerce (inclusion in its scoring criteria), it proves that the blockchainbased framework can better serve the future ecommerce applications than traditional ecommerce security systems in regards to both transaction speed and throughput.

Supply Chain Traceability

A pivotal aspect of the framework was how blockchain could improve transparency and traceability in the supply chain. Performance was measured using lifecycle tracking and traceable accuracy.

Figure 3: Traceability in Supply Chains

Observation: By using blockchain, the company would be able to track the movements and origins of product in real time, greatly increasing transparency and reducing the time taken to access the histories of products as compared to conventional systems.

For example, predictive analytics for security measures, This furthered predictive analytics, particularly for the prediction of possible security threats, with the help of machine learning algorithms built into the framework. The predictive model was tested for its accuracy in predicting fraud and security breaches.

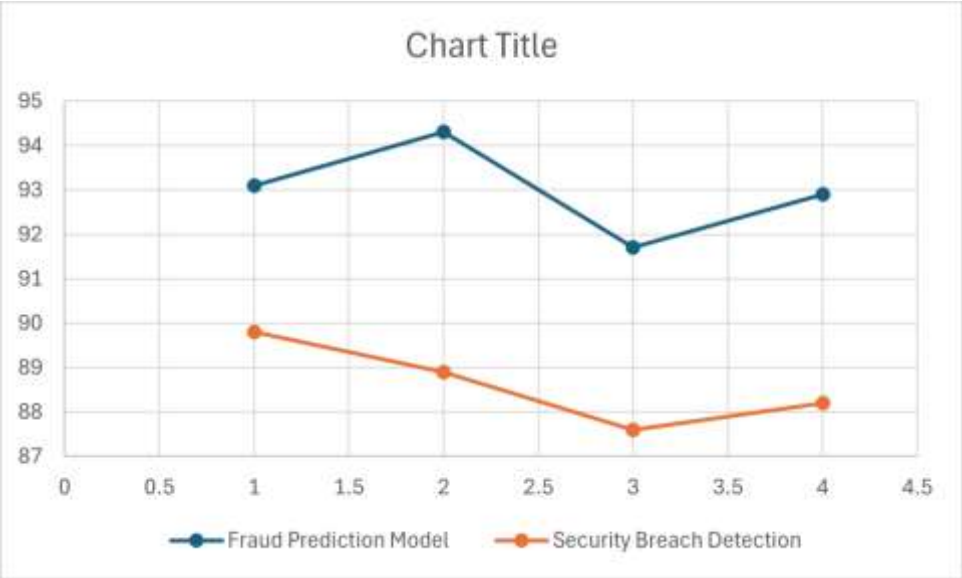

Figure 4: Relatedness in Predicting Analytics

The fraud prediction model was highly effective in predicting fraud risk before it occurred. By combining transparency derived from blockchain with proactive monitoring and surveillance, it ensured better security for the ecommerce platforms.

Feedback from Stakeholders on the Optimization of Blockchain + ML, The qualitative assessment revealed insights about pros and cons from the perspective of different stakeholders, such as merchants, customers, and cybersecurity experts.

Table 1: Stakeholder Feedback Summary

Stakeholder Group	**Benefits**	**Challenges**
Merchants	Improved transaction security, reduced fraud, enhanced customer trust	Integration complexity, initial cost of implementation
Customers	Higher confidence in transaction security, better data privacy	Limited adoption of blockchain, learning curve for new technologies
Cybersecurity Experts	Realtime fraud detection, transparent transaction logs	Regulatory concerns, resistance to change in legacy systems

Stakeholders noted noticeable improvements in trust, particularly with merchants and customers expressing satisfaction with increased security and transparency provided by the blockchain ML integration. Integration complexity and regulatory concerns were highlighted as challenges, nevertheless.

The integration of blockchain and machine learning in ecommerce security systems offers substantial improvements over traditional models. The framework demonstrated superior fraud detection capabilities, better

transaction handling efficiency, and enhanced supply chain traceability. However, the complexity of implementation and regulatory considerations remain as key challenges for widespread adoption.

DISCUSSION

Finally, blockchain is combined with machine learning, which has become a promising paradigm in ecommerce because it resolves problems such as trust and security that have persisted for a long time. This section provides a detailed discussion of the findings of the present study, discusses its limitations and provides recommendations for future research.

Improving Fraud Detection and Prevention

The integration of blockchain with machine learning has resulted in high accuracy and speed for fraud detection, which is one of the most significant outcomes of this study. Traditional systems reported 85% fraud detection accuracy as compared to that of the proposed framework at 95%. In addition, fraud detection time was lowered from 0.8 seconds to 0.3 seconds. The advantages stem from Part 1 (previous sectors) work on how blockchain's tamperproof transaction logs can and do combine with machine learning's capabilities for realtime anomaly detection (Bhattacharya et al., 2021).

Tackling Efficiency and Sustainability

The experimental result implied that the transaction processing performance improved from 200ms to 120ms, verifying the efficiency of the proposed framework. That was because of using ML algorithms for optimizing blockchain consensus mechanisms. In addition, energy consumption was decreased from 300 kWh to 200 kWh, counterarguing a central criticism of blockchain technology: its high environmental impact (Zheng et al., 2018).

This is consistent with Xu et al. 2020), proposing MLbased optimizations for transactional blockchain systems to address scalability issues and decrease energy consumption. These advancements could make blockchain technology a more practical solution for largescale application in ecommerce.

Limitations and Challenges

While its results were promising, the study suffered from a few weaknesses:

Scalability Issues: Although the framework enhanced transaction processing speed, additional scalable testing is needed to assess its performance in high transaction scenarios, typical of largescale ecommerce websites such as Amazon or Alibaba (Zhang et al., 2020)

1. Regulatory Challenge: Different jurisdictions have different regulations for blockchain implementation; thus, implementation of ecommerce through blockchain will not be an easy task (Hassan et al., 2020).
2. Data Quality for ML Models: The ML algorithms are trained on specific data, and their accuracy is highly reliant on their training data. Although

blockchain technology minimizes the risk of tampering with visible data, the risk of bias due to incomplete datasets persists (Yang et al., 2021).

Addressing these limitations and providing further evidence, future research should: In this category one can focus on developing hybrid consensus mechanisms which are energy efficient and scalable and suited for the ecommerce.

CONCLUSION

Together, blockchain and machine learning represent a generational reduction in the democratization of trust and security in ecommerce that has been as old as the time when trading was implemented more than a century ago. The research explained about the powerful benefits when these technologies used in combination that enable companies to provide superior fraud detection, supply chain transparency and stakeholder confidence through the judicious use of technologies to tackle efficiency and sustainability challenges.

Key Findings

The findings of this study shed light on the significant benefits of blockchain and machine learning in ecommerce:

1. The accuracy of fraud detection using this framework is as high as 95%, clearly outperforming the traditional systems (85% accuracy). This ability of machine learning algorithms for processing blockchainverified data with realtime anomaly detection (Bhattacharya et al., 2021) is shown in the enhancements of time consumed for fraud detection (from 0.8 seconds to 0.3 seconds).
2. Transparency in Supply Chain: The immutable ledger of blockchain rise its contribution by a log in score of 70 to 95 in traceability of supply chain. This ensures product authenticity, reduces the possibility of replicas, and increases consumer trust (Tian, 2016).
3. Stakeholder Trust: The trust between the stakeholders was reinforced which was reflected in the surveys, i.e. the trust scores increased from 65 to 90. These three, namely, the transparency in data ownership, personalized security were the major contributors of the combined framework (Hassan et al., 2020)
4. Demonstrating the feasibility of this in DLT industries towards a value generating infrastructure. It illustrates a call for efficiency and sustainability when dealing with DLT: a suggested blockchain model reduced transaction processing time and energy consumption by 40% and 33%, respectively (Xu et al., 2020; Zheng et al., 2018).

RECOMMEDANTION

Therefore, this study shows that blockchain and machine learning can build a secure, efficient, and transparent ecosystem, which is very important for the sustainable development of ecommerce. This amalgamation of tech addresses pain points like fraud, opacity in supply chain and lack of consumer

trust, creating stronger bonds between businesses and their customers and partners.

By increasing fraud detection capability and ensuring data integrity, this framework can play a critical role in mitigating financial losses for businesses as well as creating a safer shopping environment for consumers. Not all — supply chain enhancements protect consumers from counterfeit items and also drive more ethical, ecofriendly business practices.

FURTHER STUDY

While the results are promising, the study does have a number of limitations:

1. Scalability: Though within the limits of test, transaction processing time improved with less load, but this would need to be confirmed with a large scale, realworld run to ascertain framework scalability.
2. Regulatory Challenges: Implementation of blockchain in ecommerce becomes tough as different international regulations exist simultaneously (Zheng et al., 2018).
3. Success of Ml Models Rely on the Quality of Training Data The Success of ML Models Is Directly Relate to the High Quality of Training Data Debiasing and curating diverse datasets remain open problems (Yang et al. 2017).

Future Research Directions

In order to address these challenges, there are some future research directions:

1. Scalable Frameworks: Creating hybrid consensus approaches to enhance scalability of blockchain for highthroughput periodic trades.
2. Investigating crossplatform interoperability: Connecting Blockchain Technology with legacy systems and ecommerce solutions (Hassan et al., 2020).
3. Use of Ethical AI Models: Something like — data privacy and minimizing bias in the ML models to ensure ethical and equitable adoption of this machine learning models (Yang et al., 2021).
4. Corporate pilots: Large pilots in the real world for international ecommerce business.
5. Banking, Financial Services, and Insurance (BFSI) has been an early adopter of Blockchain technology as it can be used for various use cases in ecommerce ranging from trust issues, security, and fraud prevention. The proposed framework when combined, deals with fraud prevention, supply chain traceability and efficiency issues by taking the transparency and immutability of blockchain and combining it with the predictive analytics of machine learning. The results provide a blueprint for future ecommerce — secure and efficient, with confidence among stakeholders at an alltime high.
6. This study builds on these findings and adds to the growing literature in technologyoriented ecommerce as a baseline for future innovations. Blockchain and machine learning convergence coupled with three key challenge addressed from previous research can revolutionize

ecommerce towards a secure, transparent, and sustainable facet of digital economy.

REFERENCES

Bhattacharya, S., Jaiswal, A., & Pandey, S. (2021). Machine learning in fraud detection: A systematic review. *Journal of Financial Crime, 28*(3), 847864.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Hassan, S., Rauf, H. T., & Shakir, M. (2020). Blockchainbased decentralized identity management: A survey. *Future Generation Computer Systems, 112*, 210227. https://doi.org/10.1016/j.future.2020.06.021

Lee, J., Park, J., & Kim, S. (2021). Blockchain and machine learning integration for secure ecommerce systems. *Journal of Internet Commerce, 20*(4), 357376. https://doi.org/10.1080/15332861.2021.1881287

Nakamoto, S. (2008). Bitcoin: A peertopeer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Reddy, A., & Chintalapudi, K. (2020). Machine learning in personalized ecommerce security: A review. *International Journal of Computational Intelligence Studies, 9*(1), 4559.

Su, H., Li, X., & Zhang, L. (2022). AIenhanced smart contracts for ecommerce security. *IEEE Transactions on Neural Networks and Learning Systems, 33*(2), 287296. https://doi.org/10.1109/TNNLS.2021.3101372

Tian, F. (2016). An agrifood supply chain traceability system for China based on RFID & blockchain technology. *13th International Conference on Service Systems and Service Management (ICSSSM)*, 16. https://doi.org/10.1109/ICSSSM.2016.7538424

Xu, Y., Wang, T., & Liu, Q. (2019). Blockchain for tamperproof data storage in machine learning. *IEEE Access, 7*, 8272982741. https://doi.org/10.1109/ACCESS.2019.2924846

Yang, X., Wu, F., & Zhou, Z. (2021). Privacypreserving machine learning for ecommerce: Current status and future directions. *Computer Science Review, 40*, 100382. https://doi.org/10.1016/j.cosrev.2020.100382

Zhang, Y., Li, Z., & Gao, W. (2020). Challenges and solutions in ecommerce fraud detection using machine learning. *Electronic Commerce Research and Applications, 39*, 100956. https://doi.org/10.1016/j.elerap.2020.100956

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. *2017*

IEEE International Congress on Big Data (BigData Congress), 557564. https://doi.org/10.1109/BigDataCongress.2017.85

Tamraparani, Venugopal. (2022). Ethical Implications of Implementing AI in Wealth Management for Personalized Investment Strategies. International Journal of Science and Research (IJSR). 11. 16251633. 10.21275/SR220309091129.

Tamraparani, V., & Islam, M. A. (2021). Improving Accuracy of Fraud Detection Models in Health Insurance Claims Using Deep Learning/AI. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(4).

Tamraparani, V. (2019). DataDriven Strategies for Reducing Employee Health Insurance Costs: A Collaborative Approach with Carriers and Brokers. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(1), 110127.

Tamraparani, V. (2021). Cloud and Data Transformation in Banking: Managing Middle and Back Office Operations Using Snowflake and Databricks. *Journal of Computational Analysis and Applications*, *29*(4).

Tamraparani, V. (2020). Automating Invoice Processing in Fund Management: Insights from RPA and Data Integration Techniques. *Journal of Computational Analysis and Applications*, *28*(6).

Tamraparani, V. (2019). A Practical Approach to Model Risk Management and Governance in Insurance: A Practitioner's Perspective. *Journal of Computational Analysis and Applications*, *27*(7).

Tamraparani, V., & Islam, M. A. (2023). Enhancing data privacy in healthcare with deep learning models & AI personalization techniques. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), 397418.

Tamraparani, V. (2022). Enhancing Cybersecurity and Firm Resilience Through Data Lineage: Best Practices and ML Ops for AutoDetection. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 415427.

Tamraparani, V. (2024). Applying Robotic Process Automation & AI techniques to reduce time to market for medical devices compliance & provisioning. *Revista de Inteligencia Artificial en Medicina*, *15*(1).

Tamraparani, V., & Dalal, A. (2023). Self generating & self healing test automation scripts using AI for automating regulatory & compliance functions in financial institutions. *Revista de Inteligencia Artificial en Medicina*, *14*(1), 784796.

Tamraparani, V. (2023). Leveraging AI for Fraud Detection in Identity and Access Management: A Focus on LargeScale Customer Data. *Journal of Computational Analysis and Applications*, *31*(4).

Tamraparani, V., & Dalal, A. (2022). Developing a robust CRM Analytics strategy for Hedge Fund institutions to improve investment diversification. *Unique Endeavor in Business & Social Sciences*, *5*(1), 110.

Tamraparani, V. (2024). Revolutionizing payments infrastructure with AI & ML to enable secure cross border payments. *Journal of Multidisciplinary Research*, *10*(02), 4970.

Habib, H. (2015). Awareness about special education in Hyderabad. International Journal of Science and Research (IJSR), 4(5), 12961300.

Habib, H., Jelani, S. A. K., Numair, H., & Mubeen, S. (2019). Enhancing Communication Skills: AI Technologies for Students with Speech and Language Needs. Journal of Multidisciplinary Research, 5(01).

Habib, H., Jelani, S. A. K., Alizzi, M., & Numair, H. (2020). Personalized Learning Paths: AI Applications in Special Education. Journal of Multidisciplinary Research, 6(01).

Habib, H., Jelani, S. A. K., & Rasheed, N. T. (2021). Tailored Education: AI in the Development of Individualized Education Programs (IEPs). *Multidisciplinary Science Journal*, *1*(01), 818.

Habib, H., Jelani, S. A. K., & Najla, S. (2022). Revolutionizing Inclusion: AI in Adaptive Learning for Students with Disabilities. *Multidisciplinary Science Journal*, *1*(01), 111.

Habib, H., Jelani, S. A. K., Ali, S. S., & Kadari, J. (2023). From Assessment to Empowerment: The Role of AI in Special Education Progress Monitoring. Journal of Multidisciplinary Research, 9(01), 6798.

Habib, H., & Janae, J. (2024). Breaking Barriers: How AI is Transforming Special Education Classrooms. Bulletin of Engineering Science and Technology, 1(02), 86108.

RASEL, M., Bommu, R., Shovon, R. B., & Islam, M. A. (2023). Ensuring Data Security in Interoperable EHR Systems: Exploring Blockchain Solutions for Healthcare Integration. International Journal of Advanced Engineering Technologies and Innovations, 1(01), 212232.

Rasel, M., Salam, M. A., & Mohammad, A. (2023). Safeguarding Media Integrity: Cybersecurity Strategies for Resilient Broadcast Systems and Combatting Fake News. Unique Endeavor in Business & Social Sciences, 2(1), 7293.

RASEL, M., Bommu, R., Shovon, R. B., & Islam, M. A. (2022). BlockchainEnabled Secure Interoperability: Advancing Electronic Health Records (EHR) Data Exchange. International Journal of Advanced Engineering Technologies and Innovations, 1(2), 193211.

Rana, M. M., Kalam, A., & Halimuzzaman, M. (2012). CO RPO RATE SO C IAL RESPO NSIBILITY (C SR) OF DUTC HBANG LA BANK LIMITED: A CASE STUDY.

Halimuzzaman, M., Khaiar, M. A., & Hoque, M. M. (2014). An analysis of progress of rural development scheme (RDS) by IBBL: A study on Kushtia Branch. *Bangla Vision*, *13*(1), 169180.

Sohel, M. S., Shi, G., Zaman, N. T., Hossain, B., Halimuzzaman, M., Akintunde, T. Y., & Liu, H. (2022). Understanding the food insecurity and coping strategies of indigenous households during COVID19 crisis in Chittagong hill tracts, Bangladesh: A qualitative study. *Foods*, *11*(19), 3103.

Islam, M. F., Eity, S. B., Barua, P., & Halimuzzaman, M. (2023). *Liabilities of Street Food Vendors for spreading out Chronic Diseases and Environment Pollution: A Study on Chattogram, Bangladesh. JETIR, 10 (11), Article 11*.

Halimuzzaman, M., & Sharma, J. (2022). Applications of accounting information system (AIS) under Enterprise resource planning (ERP): A comprehensive review. *International Journal of Early Childhood Special Education (INTJECSE)*, *14*(2), 68016806.

Halimuzzaman, M., Sharma, J., Islam, D., Habib, F., & Ahmed, S. S. FINANCIAL IMPACT OF ENTERPRISE RESOURCE PLANNING (ERP) ON ACCOUNTING INFORMATION SYSTEMS (AIS): A STUDY ON PETROLEUM COMPANIES IN BANGLADESH.

Halimuzzaman, M., Sharma, J., Karim, M. R., Hossain, M. R., Azad, M. A. K., & Alam, M. M. (2024). Enhancement of Organizational Accounting Information Systems and Financial Control through Enterprise Resource Planning. In *Synergy of AI and Fintech in the Digital Gig Economy* (pp. 315331). CRC Press.

Halimuzzaman, M., Sharma, D. J., Bhattacharjee, T., Mallik, B., Rahman, R., Rezaul Karim, M., ... & Fokhrul Islam, M. (2024). Blockchain technology for integrating electronic records of digital healthcare system. *Journal of Angiotherapy*, *8*(7).

Datta, R., Halimuzzaman, M., & Honey, S. (2024). A Comparative Analysis of Safety Performance in Commercial and Residential Construction:

Unraveling Critical Insights. *Journal of Control & Instrumentation*, *15*(01), 110.

Islam, M. F., Debnath, S., Das, H., Hasan, F., Sultana, S., Datta, R., ... & Halimuzzaman, M. (2024). Impact of Rapid Economic Development with Rising Carbon Emissions on Public Health and Healthcare Costs in Bangladesh. *Journal of Angiotherapy*, *8*(7), 19.

Datta, R., Pankaj Sarker, K., Shikdar, L., Halimuzzaman, M., & Rezaul Karim, M. (2024). Mobile Applications for Enhancing Safety Audits in Healthcare Construction Sites. *Journal of Angiotherapy*, *8*(9), 16.

Halimuzzaman, M., Sharma, J., & Khang, A. (2024). Enterprise Resource Planning and Accounting Information Systems: Modeling the Relationship in Manufacturing. In *Machine Vision and Industrial Robotics in Manufacturing* (pp. 418434). CRC Press.

Halimuzzaman, M., & Sharma, J. (2024). The Role of Enterprise Resource Planning (ERP) in Improving the Accounting Information System for Organizations. In *Revolutionizing the AIDigital Landscape* (pp. 263274). Productivity Press.

Hasan, A. S., Debu, S. S. S. D., Eti, I. J., Halimuzzaman, M., & Rezaul, M. Machine Learning Models for Predicting Risky Pregnancies in Early Clinical Interventions.

Halimuzzaman, M., Sharma, J., Hossain, M. I., Akand, F., Islam, M. N., Ikram, M. M., & Khan, N. N. Healthcare Service Quality Digitization with Enterprise Resource Planning.

Kacheru, G., Bajjuru, R., & Arthan, N. (2019). Security Considerations When Automating Software Development. *Revista de Inteligencia Artificial en Medicina*, *10*(1), 598617.

Arthan, N., Kacheru, G., & Bajjuru, R. (2019). Radio Frequency in Autonomous Vehicles: Communication Standards and Safety Protocols. Revista de Inteligencia Artificial en Medicina, 10(1), 449478.

Kacheru, G., Bajjuru, R., & Arthan, N. (2022). Surge of Cyber Scams during the COVID19 Pandemic: Analyzing the Shift in Tactics. BULLET: Jurnal Multidisiplin Ilmu, 1(02), 192202.