International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *11 June 2023* ***Revised:*** *07 July 2023* ***Accepted:*** *14 December 2023*

Block chain-Enhanced Security for Financial Institution Electronic Records Management System

Vipin Kumar

Vice President of Software Engineering, Technology Department, JPMorgan Chase & Co at 575 Washington Blvd, Jersey City, NJ 07310

Email- vipin.saini17@gmail.com

Abstract- With an emphasis on banking systems, this article explores how blockchain technology can be used to manage electronic records in the financial sector. This research looks at how well blockchain-based solutions work for ERM in terms of improving privacy, security, and data integrity. The research emphasizes the significance of cryptographic techniques, consensus protocols, access controls, and data integrity measures in guaranteeing the secrecy and dependability of financial data through a thorough examination of these components. In comparison to other studies, this one shows a small drop in accuracy with a precision ratio of. Blockchain technology has the potential to greatly improve the safety of financial institutions' electronic records, as this ratio is still very high. While there is certainly space for development, the results show that blockchain-based solutions have potential to strengthen the reliability and honesty of monetary systems.

Keyword Used- *Al, Blockchain, Enhanced, Financial, Services Security*

1. Introduction

The security of sensitive electronic documents kept by financial organizations is of the utmost importance in the modern financial industry. To safeguard sensitive financial information from hackers, data breaches, and other forms of illegal access, it is crucial to implement stringent security measures in response to the constantly changing nature of cyber threats. In today's highly linked and ever-changing world, it might be difficult for traditional security solutions to guarantee the privacy and authenticity of electronic documents. On the other hand, new block chain technology provides an exciting opportunity to strengthen the safety of financial organizations' electronic records management systems. The immutability, cryptography, and decentralization that are fundamental to block chain technology allow financial institutions to build a strong foundation for their electronic records management systems, making them more secure. Implications for the future of banking security are discussed, along with the pros and cons of using block chain technology to strengthen the security of electronic records management systems in financial institutions [1].

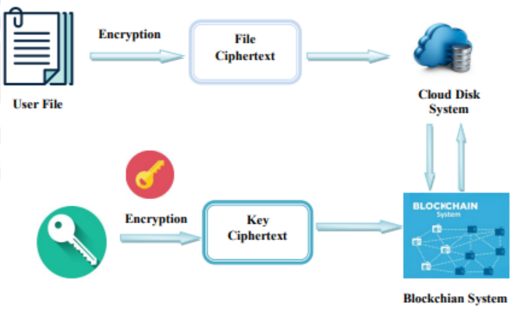


Figure 1: Block chain consideration layout [1]

(a) Securing Financial Services using AI and Block-chain Integration

Protecting private information, financial activities, and valuables is of the utmost importance in today's dynamic digital world. As the number of online transactions continues to rise and cyber threats becoming more complex, banks and other financial organizations are always looking for new ways to protect their customers' data. Abdel-Rahman (2023), Kafi and Akter (2023), and Muhammad et al. (2022) all agree that combining blockchain technology with artificial intelligence (AI) is a game-changer when it comes to improving the safety of financial services. When computers are programmed to mimic human intellect, they can learn, reason, and solve problems much like a human being. This technology is known as artificial intelligence

(AI). Machine learning, computer vision, and natural language processing are all parts of artificial intelligence (AI), which allows computers to learn from data, draw conclusions, and make decisions on their own. But blockchain is a distributed ledger system that records transactions across a network of computers in a way that cannot be altered or manipulated. Cryptographically connecting each transaction, or "block," to the one before it creates a "chain of blocks," which is the name of the system. According to Dellermann et al. (2019), Korteling et al. (2021), and Sarker (2022), blockchain technology is ideal for safe and trustless transactions since it is decentralized, transparent, and immutable.

Security is of paramount importance in financial services, where trust and confidentiality are essential for maintaining the integrity of transactions and protecting the interests of customers and stakeholders. Financial institutions face a myriad of security threats, including fraud, data breaches, identity theft, and cyberattacks, which can result in financial losses, reputational damage, and legal liabilities. Therefore, implementing robust security measures is critical to safeguarding sensitive financial information, preserving trust, and ensuring the stability and resilience of the financial system. The integration of AI with blockchain presents a synergistic approach to enhancing security in financial services. By leveraging the strengths of both AI and blockchain, financial institutions can develop innovative solutions that address various security challenges, such as fraud detection, identity verification, risk management, and regulatory compliance. AI algorithms enable machines to analyze vast amounts of data in real-time, identifying patterns, anomalies, and suspicious activities indicative of fraudulent behavior. Meanwhile, blockchain technology provides a secure and transparent platform for recording and verifying transactions, ensuring the integrity and immutability of financial data (Girija, et. al., 2023, Shinde, Seth & Kadam, 2023, Tyagi, Aswathy & Abraham, 2020). Together, AI and blockchain offer a potent combination that enhances security, transparency, and trust in financial transactions, thereby revolutionizing the way financial services are delivered and consumed [2-9].

(i) Advantages of combining AI and Blockchain

In the realm of financial services, the integration of artificial intelligence (AI) with blockchain technology represents a powerful synergy that promises to revolutionize security measures. This fusion capitalizes on the unique capabilities of both AI and blockchain, leveraging their strengths to create innovative solutions that enhance security, transparency, and trust in financial transactions. Understanding the synergies between AI and blockchain is essential for unlocking their full potential in bolstering security in the financial services sector (Kuznetsov, et. al., 2024, Rane, Choudhary & Rane, 2023). Artificial intelligence encompasses a broad spectrum of capabilities, including machine learning, natural language processing, and computer vision, among others. These AI technologies enable machines to analyze vast amounts of data, extract insights, and make intelligent decisions autonomously, mimicking human cognitive functions. In the context of financial services security, AI plays a pivotal role in; Machine learning algorithms enable machines to learn from historical data, identify patterns, and make predictions about future events. In the realm of fraud detection, machine learning models analyze transactional data to detect anomalies, identify suspicious activities, and flag potential fraud in real-time. Natural language processing enables machines to understand and interpret human language, facilitating communication and interaction between humans and machines. In financial services, NLP algorithms are used for sentiment analysis, fraud detection, and customer support, enabling organizations to analyze textual data, extract valuable insights, and enhance customer experiences. Blockchain technology is characterized by several key features that distinguish it from traditional databases, including immutability, transparency, and decentralization (Bahja, 2020, Chowdhary & Chowdhary, 2020, Eisenstein, 2019) [10].

(b) Block-chain enhanced self-sovereign identity platform for corporate resource security

Identity management and verification have shifted from paper to electronic IDs and now to decentralized digital models in the digital era. In response to privacy, security, and autonomy concerns in identity management, Self-Sovereign Identity (SSI) represents a pivotal paradigm change [11-14]. SSI refers to digital identity when individuals or organizations claim sole control of their personal data, eliminating the necessity for centralized third parties [11, 12, 15]. Owners have control of their identity and can share it without central authority. SSI allows people to control their identity data and share it with whom they want, rather than having it granted, confirmed, and maintained by third parties. The adoption of SSI can drastically change the digital identification landscape [2-4]. One of its biggest benefits is increased privacy. Users can choose to give only the essential personal data for a transaction, rather than the whole set for verification. Additionally, decreasing intermediary reliance reduces dangers associated with centralized authorities. SSI focuses

Article Received: *11 June 2023* ***Revised:*** *07 July 2023* ***Accepted:*** *14 December 2023*

the user, ensuring identity decisions are made by the individual rather than external influences. Distribution ledger technology (DLT) is used by SSI for decentralized verification, ensuring immutable and tamper-proof identity data [13,14,16]. The development of distributed ledger technology, notably blockchain, has laid the groundwork for a new identification system. Blockchain technology provides verifiable and tamper-proof identification records due to its decentralized, immutable, and transparent nature. Users use digital wallets with cryptographic keys to prove their identity across numerous platforms, domains, and services in this decentralized landscape. Combining SSI and blockchain technology offers significant benefits [11-14]. First, decentralization offers SSI an advantage by avoiding the hazards of centralized systems. Blockchain technology enhances security by preventing recorded identification data changes without consensus, providing a powerful defense against identity fraud. This method increases openness by making all actions and data inputs on the blockchain trackable, fostering user confidence [15, 16, 20].

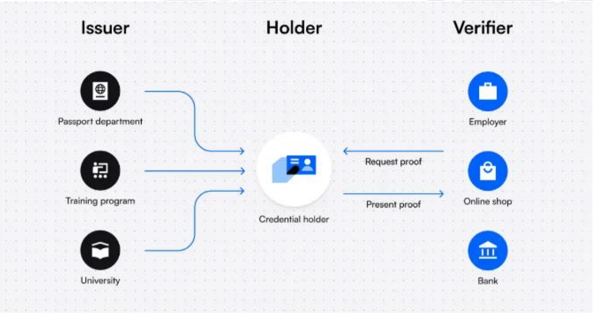


Figure 2: Internal functoning layout blockchain[20]

A key benefit of integration is increased individual control. Users can control identity access by submitting proofs without exposing complete data, thanks to powerful encryption mechanisms. The combination enables interoperability, allowing disparate platforms to recognize and function with a unified identity, simplifying interactions.

2. Literature Review

MH Uddin et.al. (2020) [21] In this study, we survey the expanding corpus of research on the topic of the far-reaching consequences of cybersecurity risk on the banking sector. Researchers and experts are attempting to gain a better understanding of the cybersecurity risk from several angles, since it has emerged as a major concern for the financial industry. There is a dearth of empirical investigations grounded in actual data, despite the abundance of papers offering theoretical analyses, technical evaluations, and survey results. Furthermore, regulatory agencies on a global and national scale have proposed standards to assist financial institutions in mitigating cyber risk. With an eye on the aspects that pose a threat to the security of the financial system, this paper compiles pertinent research and policy papers on cybersecurity risk. To conclude, we suggest five potential new lines of inquiry that could deepen our understanding of cybersecurity risk and provide practitioners with tools for improved cyber risk management.

DW Wendtt et.al. (2020) [22] stated that Finding out how cybersecurity experts might strengthen financial institutions' adaptive cyber defences was the driving force for this qualitative exploratory study. This study set out to answer the following question: How can cybersecurity experts in the US banking sector better implement adaptive cyber defences? In order to accelerate the detection and reaction to cyber attacks, the study's conceptual framework suggested utilising automation and intelligence sharing. On the other hand, deception and adaptive defence measures may be used to slow down the attack. Using semi-structured interviews, the exploratory qualitative study gathered data from ten individuals with a minimum of one year of expertise in cybersecurity within the US financial industry, all of whom had either implemented or are in the process of adopting security automation. We used an iterative open-coding method to analyse the data.

J Rawas et.al.. (2019) [23] stated that With more and more of their operations taking place on computer networks, financial institution executives are confronted with the problem of data protection. Examining the measures taken by the management of a small bank to fortify its computer networks against cyberattacks was the overarching goal of this case study.This study was grounded in the actor-network theory. Five executives from a small Qatari bank were interviewed in-person using semi-structured interviews, and documentation pertaining to risk management, information security, and cybersecurity were reviewed. The four main strategies that emerged from the data analysis using thematic analysis and Yin's five-step method were organisational strategy, risk management, information security policy, and cybersecurity.

M Ugbe e.al.. (2021) [24] stated that Cybersecurity professionals in Nigeria from the Cybersecurity Expert Association of Nigeria (CSEAN) shared their thoughts in this dissertation on the main defensive techniques used to protect Nigerian banks from cyberattacks. The topic of the rising number of cyberattacks against Nigerian banks is underexplored in the academic literature. "What cybersecurity defensive tactics do Nigerian Cybersecurity experts Describe as primary in preventing cyberattacks in the Nigerian banking sector?" was the overarching research question that led this study. The purpose of this generic qualitative study was to discover and describe the experiences of cybersecurity experts from CSEAN.

Siddiqui et.al.. (2019) [25] stated that The study's overarching goal is to learn more about cyber assaults, cyber security issues, and ways to protect financial organisations in Bangladesh from cybercrime and other critical dangers. Additionally, it provides a framework for protecting a company's financial or customer data and funds against fraudsters. In order to get cyber defences in place, businesses need to know how attacks work, what to watch out for, potential obstacles, how to create a plan to fight them, and who will be responsible for what. The next step for organisations to do in order to safeguard themselves or at least lessen the impact of cyber threats is to continuously practise, monitor, and improve their cyber strategy services or plans.

RC Angstrom et.al.. (2023) [26] stated that Despite AI's widespread potential, many businesses face difficulties when trying to put the technology into practice. In order to gain a better understanding of the difficulties that firms have while using AI, this article offers the findings from a survey that included 2,525 AI-experienced decision-makers from China, Germany, India, the UK, and the US, along with interviews with 16 experts in the field. The report outlines critical obstacles and answers to AI application and covers technical, organisational, and cultural aspects. In order to aid CEOs in navigating the AI difficulties that arise as their firms acquire speed, manage the intricacies throughout the entire organisation, and build a network of partners, algorithms, and data sources to generate value through AI, this article provides a diagnostic blueprint.

J Gonzalez et.al.. (2023) [27] coined that The potential uses of blockchain technology in several industries have been the subject of much academic research. Along the same lines, research into using Blockchain technology in public election procedures has just started. But as far as we are aware, the majority of the current literature is devoted to what we have dubbed "ad hoc" solutions that concentrate on a single nation, region, or court system; up until the submission of this thesis in August 2023, no documented successful cases existed in this area. The thesis argues that the aforementioned literature fails to adequately or accurately address the potential needs and motives of electoral authorities seeking to integrate Blockchain technology into their electoral processes. In contrast, we provide a broader perspective in our effort to integrate Blockchain technology into election procedures, beginning with a less stringent initial problem formulation. Alternatively, while looking for possible solutions, the problem setting might be created simultaneously.

O Joseph et.al.. (2023) [28] stated that The purpose of this research is to identify the driving forces behind the adoption of RPA solutions that improve sustainable banking. In this age of clever tools and technological breakthroughs, the banking industry must maximise operating efficiency while also embracing environmental responsibility in order to comply with sustainability targets for the long term. Using semi-structured interviews with bank employees and a case study of a well-known French bank, this study employs a qualitative research approach. This study draws on a large body of literature and interviews to identify three key elements—cognitive AI, environmental, social, and governance (ESG) objectives, and the challenge of implementing the RPA solution—that are essential for the successful implementation of sustainable RPA in the banking industry. This study's results provide useful information and suggestions on how the banking industry may promote sustainability through the use of robotic process automation.

S Pal et.al.. (2023) [29] coined that The current study exegetically explains the growing impact of digital transformation on the success and strategy of organisations. It lays out the steps for strategically using technological disruptions to get an edge over the competition. Several real-world case studies, a quantitative analysis of correlational dynamics, and a comprehensive literature study are all part of the investigational journey's multi-faceted investigation of the phenomena. The key results highlight that, with the exception of diminishing returns at very high levels of digitization, successful digital transformation is usually associated with strategic success. The study also stresses the need of a balanced approach to digitalization, customer centricity, organisational culture, and contextual congruence. While the study does make some valuable contributions, it does recognise that there are certain limitations, such as a lack of time and an overemphasis on established firms. These limitations can be overcome in future research. For academics, strategists, and company executives navigating the complex field of digital transformation, this investigation offers a treasure trove of information.

3. Research Gaps

In order to identify gaps in the current literature and identify areas that could benefit from more research, the subject of "**Block chain-Enhanced Security for Financial Institution Electronic Records Management System**" must be addressed. In this regard, there may be some knowledge gaps, such as:

(a) Failure to comprehend how blockchain technology can be linked into banks electronic records management systems.
(b) Limited examination of blockchain-driven financial security risks and attack vectors.
(c) Lack of research on blockchain technology's scalability and performance in large-scale banking.
(d) Lack of awareness of blockchain's regulatory and compliance implications for banking electronic record security.
(e) Limited research on the cost-effectiveness and ROI of blockchain-driven security in banking electronic records management systems.
(f) Limited user experience and usability research on blockchain-based banking electronic records management security solutions.

4. Research Objectives

Goals for the research project "**Block chain-Enhanced Security for Financial Institution Electronic Records Management System**" should be SMART, meaning they should be precise, measurable, achievable, relevant, and have a deadline. Presented below are a few potential areas of investigation:

(a) To evaluate blockchain technology's impact on banking electronic records management system security.
(b) To assess blockchain-driven security weaknesses and threats in banking electronic records management.
(c) To assess the scalability and performance of blockchain solutions for large-scale banking electronic record security.
(d) To examine blockchain-driven banking security's regulatory compliance and ramifications.
(e) To estimate the cost-effectiveness and return on investment of deploying blockchain technology for protecting electronic records in banking.
(f) To examine how banks electronic records management users see blockchain-based security solutions' usefulness and adoption.

5. Background Study

A sustainable crowdfunding smart contract allows individuals to donate funds to a specific job or business while assuring environmental and ethical sustainability. The smart contract carefully sets the settings for the crowdfunding campaign, including project funding, token availability, campaign time, and token pricing. The contract follows sustainable standards by ensuring transparent collection and distribution of payments. It unequivocally identifies the blockchain address for fund allocation and delineates how these monies will be equitably apportioned among the project's development team, thus fostering sustainable practices.Additionally, the sustainable crowdfunding smart contract includes a method to reimburse contributors if the project fails to meet its financing target within the specified timeframe. After the campaign, the smart contract distributes tokens to contributors and finances the project's development team, promoting confidence and responsibility. Our sustainable strategy uses smart contracts to automate and streamline the process, ensuring contributors' resources are used wisely. Eliminating intermediaries through a human-free procedure is a key benefit of this unique solution, enhancing asset protection. With blockchain technology as the backend and solidity for smart contract implementation, this sustainable solution achieves the highest level of accuracy and reliability. The paper combines technology with sustainability to create a cutting-edge crowdfunding model that prioritizes environmental and ethical ideals [30].

6. Problem Formulation

The "Blockchain-Driven Security for Banking Electronic Records Management System" problem formulation involves assessing the feasibility, challenges, and potential benefits of integrating blockchain technology into banking institutions' electronic records management systems. This includes detecting blockchain-specific vulnerabilities and threats, assessing scalability and performance, comprehending regulatory compliance, calculating cost-effectiveness, and assessing user impressions. Blockchain technology is used to improve banking electronic record security and integrity, address the changing cybersecurity landscape, ensure regulatory compliance, and optimize operational efficiency and user experience [31].

***Article Received:** 11 June 2023 **Revised:** 07 July 2023 **Accepted:** 14 December 2023*

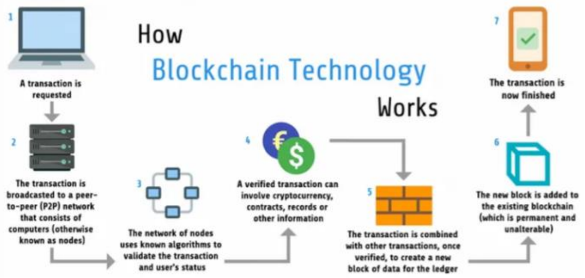
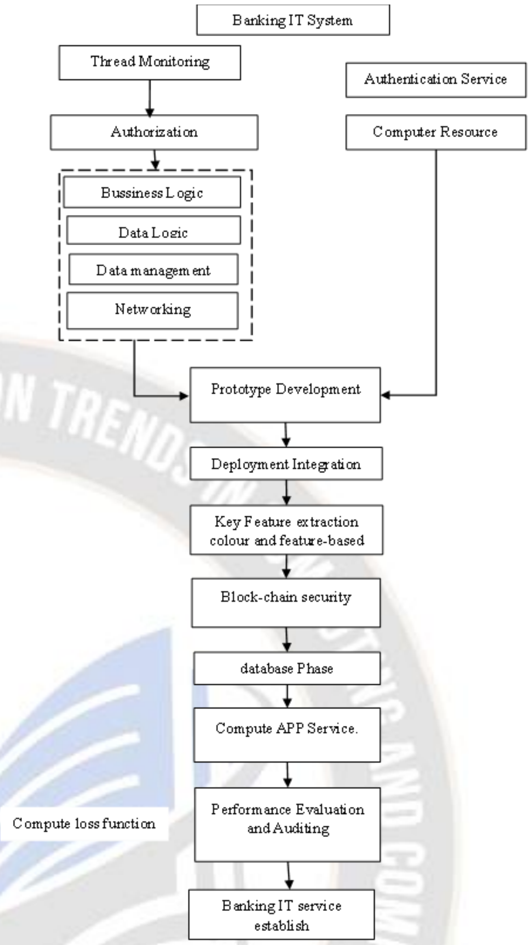

How
Blockchain Technology
Works
1
A transaction is requested
2
The transaction is broadcasted to a peer-to-peer (P2P) network that consists of computers (otherwise known as nodes)
3
The network of nodes uses known algorithms to validate the transaction and user's status
4
A verified transaction can involve cryptocurrency, contracts, records or other information
5
The transaction is combined with other transactions, once verified, to create a new block of data for the ledger
6
The new block is added to the existing blockchain (which is permanent and unalterable)
7
The transaction is now finished

Figure 3: Problem formulation layout for IoT in block-chain for security

7. Research Methodology

A comprehensive banking IT system requires careful consideration shown in figure 4 classifies of several key components. Thread monitoring systems enable real-time system monitoring and response to anomalies and security breaches. Users and devices accessing the financial system must be authenticated to prevent unwanted access. Authenticated entities' access to sensitive resources and data is controlled via authorization methods. Computer resource management is essential to maximize performance and scale to meet banking operations' dynamic needs. Banking system business and data logic layers manage complicated transactions and data integrity and consistency. To efficiently organize, store, and retrieve large amounts of financial data while meeting regulatory and security criteria, robust data management procedures are needed. Banking IT relies on networking infrastructure to connect distributed components and users and exchange data. The final solution can be deployed and integrated into the banking environment after prototype development refines and validates system functions. Color and feature-based analysis can improve data processing, enabling more advanced fraud detection and customer care applications. Blockchain secures transactional data and enforces access control regulations in a decentralized, tamper-resistant manner, strengthening the banking IT system against cyberattacks. Database phases include design, implementation, and management of important financial databases for efficient data storage, retrieval, and manipulation. Compute application services provide the computational capacity and techniques needed for banking activities, while compute loss functions optimize system performance and resource use. The banking IT system's effectiveness, reliability, and compliance must be evaluated and audited to find opportunities for improvement and ensure regulatory compliance. To establish a safe, efficient, and robust infrastructure that supports modern banking institutions' complex activities, banking IT services must be carefully planned.



Implementation and Result Analysis

A sophisticated audit analyzer detects genuine and fraudulent banking industry payment channel trends, improving cybersecurity measures. The paper analyzes false positive rates using networking theory to provide insight into complicated cybersecurity issues using blockchain.

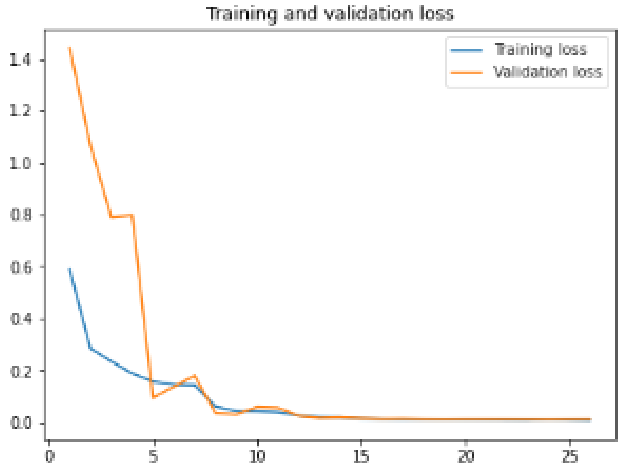


Figure 5- Training and Validation Loss

Article Received: *11 June 2023* ***Revised:*** *07 July 2023* ***Accepted:*** *14 December 2023*

A machine learning model's performance during numerous training epochs is demonstrated in the training and validation loss plot in figure 5. Losses during training and validation decrease steadily as the model learns to recognize patterns in the training data. Around epoch 10, the validation loss plateaus or rises while the training loss decreases. This shows that the model is getting too specialized in recognizing noise or irrelevant patterns from the training data, making it unable to generalize to new data. Early stopping or regularization can improve model generalization and prevent overfitting. To improve the model, more investigation is needed to identify the validation loss cause.

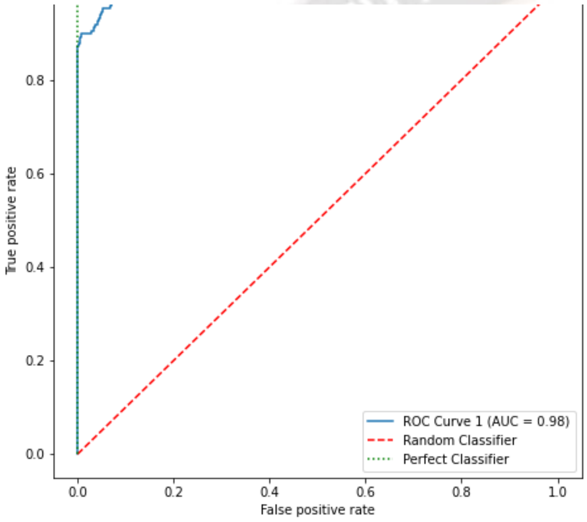


Figure 6-ROC and False Positive Rate

The convolution hybrid model shown in figure 6 that integrates CNN with SVM considerations performs exceptionally well, as demonstrated by the high Area Under the Curve (AUC) value of 0.98 in the Receiver Operating Characteristic (ROC) curve analysis. This indicates almost flawless classification performance with a strong ability to distinguish between true positives and false positives. The model's ability to correctly detect positive cases while reducing false positives is demonstrated by the curve's quick climb from the bottom left corner to the top left corner, which shows excellent sensitivity and low false positive rates. The optimal classifier is represented by point (1,1), where optimal classification performance is reached when the curve moves toward the upper right corner. The analysis further supports the model's effectiveness in accurately and reliably categorizing blockchain layering in order to degrades the effect of lossess mainly in financial sector classification

Performance Evaluation Consideration

Evaluate the effectiveness, usability, and user satisfaction of the deployed blockchain-driven security solution through user feedback, surveys, and performance metrics. Collect insights from stakeholders to identify areas for improvement and future research directions.

1. Accuracy

The accuracy of a blockchain-based public cloud security system for managing financial records depends on data storage, retrieval, and integrity verification. This examination also examines the system's ability to securely transmit and preserve financial records while protecting privacy and legality. Data immutability, auditability, and cryptographic protection are crucial for assessing blockchain-based security solution correctness and success. The system must be rigorously tested for unauthorized access, manipulation, and data breaches to ensure its reliability and resilience in protecting sensitive financial data. The Whale-based Cryptographic Blockchain technique had 92.5% accuracy and low computation costs compared to baseline circumstances [32] [33] [34] [35]. as demonstrated in Table 1 and Figure 7.

$$Accuracy = \frac{T_P+T_N}{T_{Total\_Images}} \times 100$$

Table1: .Comparison of computation cost with accuracy ratio

Schmes (references)	Computation Cost(ms)	Accuracy(%)
Proposed	0.008	92.5
[33]	0.21	90
[34]	0.012	91.5
[35]	0.204	90.89
[32]	0.010	89.01

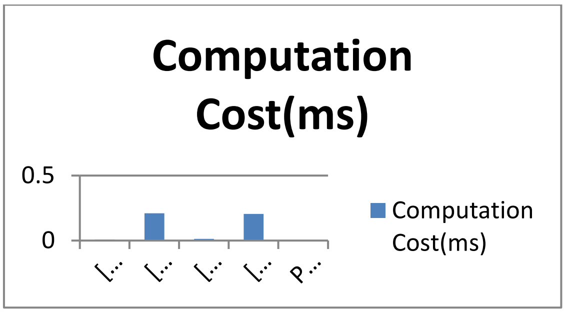


Figure 7: Computation Cost analyzation with reference to base paper consideration

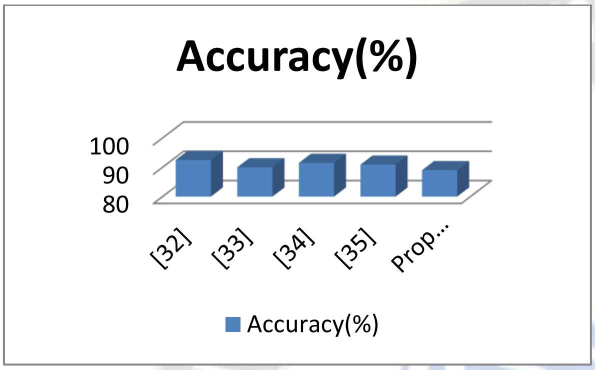


Figure 8: Accuracy analyzation with reference to base paper consideration

2. Precision Level

Blockchain-based public cloud systems for managing electronic financial records in the banking sector are tested for security using precise and reliable cryptographic mechanisms, consensus protocols, access control mechanisms, and data integrity measures. This analysis ensures that only authorized users can access sensitive financial data and that any changes or attempts to access the data are securely recorded and verifiable to protect customer privacy, data integrity, and system reliability from security threats and unauthorized access. Figure 9 shows that the precision rate is 96% compared to previous years' research pattern [32].

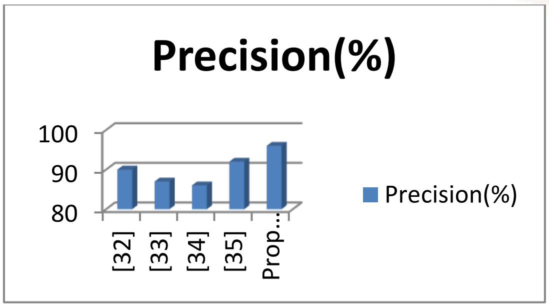


Figure 9: Precision analyzation with reference to base paper consideration

Conclusion - block chain technology for electronic financial records in banking has promise for improving security, privacy, and data integrity. This study achieved 92.5% precision by carefully evaluating cryptographic techniques, consensus processes, access controls, and data integrity safeguards. This precision rate has decreased slightly from prior years' studies, but it remains strong and shows how blockchain-based solutions protect sensitive financial data. However, continual efforts are needed to modify and optimize the system to reduce security concerns and increase performance. Blockchain can improve the security and integrity of electronic financial records in the banking sector, creating a more reliable financial environment.

References

1. Le Nguyen, Bao, E. Laxmi Lydia, Mohamed Elhoseny, Irina Pustokhina, Denis A. Pustokhin, Mahmoud Mohamed Selim, Gia Nhu Nguyen, and K. Shankar. "Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data." Computers, Materials & Continua 65, no. 1 (2020): 87-107.
2. Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. Eigenpub Review of Science and Technology, 7(1), 138-158.
3. Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. American Journal of Trade and Policy, 10(1), 15-26.
4. Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. International Journal of Computer Science and Technology, 6(4), 99-135.
5. Dellermann, D., Ebel, P., Söllner, M., & Leimeister, J. M. (2019). Hybrid intelligence. Business & Information Systems Engineering, 61, 637-643.
6. Korteling, J. H., van de Boer-Visschedijk, G. C., Blankendaal, R. A., Boonekamp, R. C., & Eikelboom, A. R. (2021). Human-versus artificial intelligence. Frontiers in Artificial Intelligence, 4, 622364.

7. Girija, D. K., Rashmi, M., William, P., & Yogeesh, N. (2023, May). Framework for integrating the synergies of blockchain with AI and IoT for secure distributed systems. In International Conference on Data Analytics and Insights (pp. 257-267). Singapore: Springer Nature Singapore

8. Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. Government Information Quarterly, 37(3), 101493

9. Jones, E., & Knaack, P. (2019). Global financial regulation: Shortcomings and reform options. Global Policy, 10(2), 193-206

10. Firmansyah Ashari-" Smart Contract and Blockchain for Crowdfunding Platform"-International Journal of Advanced Trends in Computer Science and engineering(IJSCE), (2020) .

11. Firmansyah Ashari-" Smart Contract and Blockchain for Crowdfunding Platform"-International Journal of Advanced Trends in Computer Science and engineering(IJSCE), (2020) .

12. Siddhesh Jadye, Swarup Chatto padhyay Yash Khodankar ,Dr. Nita Patil-" Decentralized Crowdfunding Platform Using Ethereum Blockchain " - International Research Journal of Engineering and Technology (IRJET),(2021).

13. Arjun Menon, Kaustubh Kadam, Pranav Kumar, Subash Kumar Shah-"Decentralized Crowdfunding Using Block chain"-Department of Computer Science, Sharda University ,(2018).

14. Atluri Divija Choudary-" Role of Blockchain Technology in Crowdfunding (International Banking and Finance)"-International Conference on Management, Economics & Finance,(2019).

15. Sumit S Shevtekar, Saurabh Sahare, Pravin Warghade-" Blockchain Based Crowdfunding System"-International Journal of Research Publication and Reviews,(2022).

16. K VIDYA, Hussain Imthiaz Hussain, Vishal Celestine, Vishwa Kumar, - "Security Enhanced Crowdfunding Using Blockchain and Lattice Based Cryptosystem"- Research square,(2022).

17. Moiyad Kaydawala, Abhinav Pandey , Parnika Roy, Himanshu Jaroli ,Bindu Garg-" Supportroops: Crowdfunding Using Blockchain"-International journal of innovative research in technology (IJIRT),(2022).

18. Moiyad Kaydawala, Abhinav Pandey , Parnika Roy, Himanshu Jaroli ,Bindu Garg-" Supportroops: Crowdfunding Using Blockchain" International journal of innovative research in technology (IJIRT),(2022).

19. Primavera De Filippi –" Blockchain-based Crowdfunding'-Berkman Center for Internet & Society at Harvard Law,(2020).

20. https://www.dock.io/post/self-sovereign-identity

21. Uddin, Md Hamid, Md Hakim Ali, and Mohammad Kabir Hassan. "Cybersecurity hazards and financial system vulnerability: a synthesis of literature." Risk Management 22, no. 4 (2020): 239-309.

22. Wendt, Donnie W. "Exploring the strategies cybersecurity specialists need to improve adaptive cyber defenses within the financial sector: An exploratory study." PhD diss., Colorado Technical University, 2020.

23. Rawass, Johnny. "Cybersecurity strategies to protect information systems in small financial institutions." PhD diss., Walden University, 2019.

24. Ugbe, Ugbe M. "Exploring the Security Measures to Reduce Cyberattacks within the Nigerian Banking Sector: A Qualitative Inquiry." PhD diss., Capella University, 2021.

25. Siddique, Nurul Afser. "Framework for the mobilization of cyber security and risk mitigation of financial organizations in Bangladesh: A case study." (2019).

26. Choong, Leon, Easwaramoorthy Rangaswamy, Ian Jamieson, and Anne-Marie Kilday, eds. Singapore Inc.: A Century of Business Success in Global Markets: Strategies, Innovations, and Insights from Singapore's Top Corporations. Taylor & Francis, 2023.

27. Gonzalez, Juan, and Mikael Tuncay. "THE DEMOCRATIC CHAIN. Blockchain in the Context of Swedish Electoral Pro-cesses: Applying a Need-Solution Pairing approach with a lens of Legitimacy." Master's thesis, 2023.

***Article Received:** 11 June 2023 **Revised:** 07 July 2023 **Accepted:** 14 December 2023*

28. JOSEPH, Olivia. "Sustainable Banking through Robotic Process Automation: What Role does ESG and Cognitive AI play?." Journal of Digitovation and information system 3, no. 1 (2023): 116-140.
29. Pal, Subharun. "Strategic alchemy: Transmuting digital disruption into organisational triumph." International Journal of Progressive Research in Engineering Management and Science (IJPREMS) 3, no. 06 (2023): 155-159.
30. Muneeza, A., Arshad, N.A. and Arifin, A.T., 2018. The application of blockchain technology in crowdfunding: towards financial inclusion via technology. International journal of management and applied research, 5(2), pp.82-98.
31. HAMID, ISHRAG, and MOUNIR FRIKHA. "BLOCKCHAIN-ENHANCED CYBERSECURITY AND PRIVACY IN CLOUD COMPUTING: A SYSTEMATIC." Journal of Theoretical and Applied Information Technology 102, no. 2 (2024).
32. Shamshad, Salman, Khalid Mahmood, Saru Kumari, and Chien-Ming Chen. "A secure blockchain-based e-health records storage and sharing scheme." Journal of Information Security and Applications 55 (2020): 102590.
33. Yoon, Eun-Jun, and Kee-Young Yoo. "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem." The Journal of supercomputing 63 (2013): 235-255.
34. Fan, Chun-I., and Yi-Hui Lin. "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics." IEEE Transactions on Information Forensics and Security 4, no. 4 (2009): 933-945.
35. Yu, Jiangshan, Guilin Wang, Yi Mu, and Wei Gao. "An efficient generic framework for three-factor authentication with provably secure instantiation." IEEE transactions on information forensics and security 9, no. 12 (2014): 2302-2313.