Volume 13, No.1, January 2026

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

REVIEW PAPER

Available online at http://www.jgrma.com

BLOCKCHAIN-ENABLED CYBERSECURITY IN BANKING SYSTEMS: A SURVEY OF CURRENT PRACTICES

Dr. Parth Gautam
Associate Professor
Department of Computer Sciences and Applications
parth.gautam@meu.edu.in

Abstract: The fast digitalization of bank services has exposed financial institutions in the global market to such cyber threats and thus, cybersecurity has become a burning issue in the financial sector. Conventional centralized security systems can hardly handle such issues as data corruption, fraud, identity theft, and system failure in response to more advanced cyberattacks. Here, blockchain technology has risen as a viable option to improve cybersecurity of banking systems because it has a decentralized, immutable, and cryptographically secured structure. The paper is a critical analysis of blockchain-based cybersecurity in the banking industry that analyzes the basic principles of blockchain technology, cybersecurity needs in banking system, and application of blockchain in security. The paper explains the possibility of providing confidentiality and integrity of data in addition to minimizing single point of failure through the use of distributed ledger technology and cryptographic methods. It also examines the use of blockchain in securing financial transactions, enhancing fraud detection and prevention, and providing the opportunity to manage the identity with the help of Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance. The literature review outlines an in-depth research of blockchain-based security solutions, AI-based threat detection and classification of cyber threats in the banking setting. The results show that blockchain has the potential to substantially increase the levels of trust, transparency, and resilience in digital banking systems, but such issues as scalability, regulatory adherence, and large-scale usability still exist. The paper has ended by highlighting the possibilities of blockchain as a supplementary cybersecurity framework in current banking ecosystems.
Keywords: blockchain technology, cybersecurity, digital banking, fraud detection, distributed ledger technology, KYC/AML compliance

1. INTRODUCTION

The reliance on digital platforms for banking introduces a range of security challenges unique to online banking environments. Unlike traditional banking, where transactions are primarily conducted in person, online banking relies heavily on secure internet-based systems. This shift has exposed users and financial institutions to cyber threats such as phishing, malware, and man-in-the-middle attacks. Cyber threats in modern banking are diverse and can target different aspects of the banking ecosystem, from user accounts to bank servers and third-party applications integrated into the banking systems[1][2][3]. One of the primary concerns in online banking security is the susceptibility of these systems to sophisticated and evolving cyberattacks. Cybersecurity has thus become an essential focus for banks worldwide, requiring investment in advanced security measures to protect sensitive financial data. Despite efforts to secure online banking platforms, vulnerabilities in authentication methods, network connections, and outdated software create potential entry points for attackers.

Cyber security serves as physical protection by keeping society safe. No accounts for trading or security, transfer money through people who know security. Cyber security is a process designed to protect a networks and devices from external threats. Cyber security means the body of technology and practice designed to protect networks, devices etc. From attack, damage from any unauthorized access. Cyber Security is the application of technologies, processes and controls the practice of protecting system, network, programs, devices and data form cyber-attacks. Its aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, network and technologies[4][5]. Cyber security is a practice of protecting computers, services, mobile devices, electronic systems, networks and data from malicious attacks. This is also known as information technology security or electronic information security. The term is use in a variety of contexts, form business to mobile computing and can be broken down into a few general categories. Network security is a way to protect computer networks from intruders, whether they are targeted attackers or opportunistic malware[6].

Blockchain technology has come out as one of the most powerful innovation tools of the modern world especially in the financial industry owing to the powerful security and clear record of transactions[7][8]. Despite originating as an intrinsic feature of Bitcoin, this distributed ledger technology has since been adopted in various fields other than the financial one. Essentially, blockchain defines a digital ledger of transactions through a series of blocks and hence there is no need for intermediaries and possibilities of cheating[9]. The financial industry where issues such as trust, high transaction cost, and lengthy time processing, have always been a thorn in the jewel will greatly benefit from blockchain implementation.

Blockchain technology is seen as an ultimate gamechanger in the world of cybersecurity. Blockchain technology is not a replacement for AI, ML & DL techniques as AI, ML& DL is the Ist line of defence for cybersecurity[10][11], the main aim is to protect data from cyberattacks but in case even after that they manage to get in, thus need to initiate second line of defence i.e. Blockchain technology[12]. Blockchain technology is the technology on which bitcoin is based basically a technique to store information through decentralised manner, it has emerged as a promising solution to address the growing concerns of cybersecurity. It plays a crucial role

in the digital world of security with its decentralised and tamper proof structure. The principal advantage of blockchain is its use of a distributed ledger. Every transaction here is locked, encrypted and verified by a network of systems thus creating a strong defence for digital data ensuring data integrity.

1.1 Structure of the paper

The structure of this paper is the following: Section 2 describes the principles of blockchain technology, such as distributed registries and cryptographic methods. Section 3 provides information about the cybersecurity requirements in banking systems and is concerned with data protection and risk management. Section 4 elaborates on the blockchain-enabled cybersecurity application like secure transactions, fraud prevention, identity management. Section 5 provides a review of the recent literature on blockchain and cybersecurity in banking, creating an overview of the main findings and the gaps in research. Section 6 is the conclusion of the paper and proposes the directions of research in the future.

2. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

Basic concepts of the Blockchain Technology explain the basic principles upon which it is possible to conduct and execute secure, decentralized, and tamper-resistant digital transactions. Such fundamentals consist of distributed ledger technology to manage shared data, cryptography to establish integrity and authenticity, and various blockchain network models which establish access control and consensus in real-world systems.

1.2 Distributed Ledger Technology

All network nodes store the same data simultaneously, clearly defining DLT. Each computer in the network has its own copy of the digital ledger, which they must check as the transaction progresses. Although blockchains and distributed ledgers share many similarities, not every distributed ledger is a blockchain[13]. The primary difference between a blockchain and a distributed ledger is that the latter does not use blocks to keep the ledger growing.

DLT is a general protocol and structure for recording data in a distributed and secure fashion. It emphasizes the presence of a system that is controlled by a distributed network and has no central control. DLT secures data through cryptography and distributes them across the network for storage[14]. This technology is designed to establish trust between parties that do not trust each other.

This technology is divided into different subcategories according to the structure created to keep the data record. The five sub-technologies are Blockchain, Tangle, Hash graph, Side-chains, Holochain.

1.3 Cryptographic Techniques in Blockchain

Since around 2000, using crypto technology in blockchain has become a significant trend. Blockchain is a unique application paradigm that combines peer-to-peer transmission, distributed data storage, consensus procedures, digital encryption technology, and other computer technologies. Blockchain growth is encouraged and constrained by cryptography technology, and the current security issues are examined. Cryptographic techniques in Blockchain are as follows:

2.1.1 Hash Function

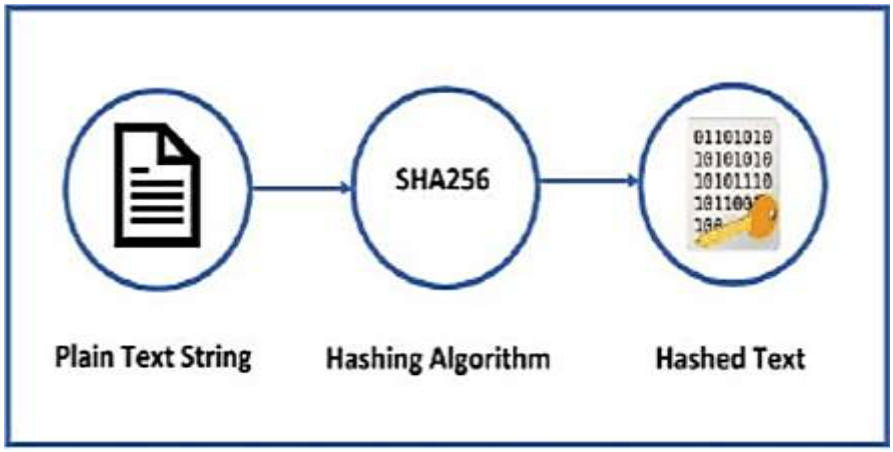

Figure: 1. Hashing Algorithm working

In Figure 1, A hash function, which is used in blockchain, is a cryptographic operation that transforms any input data, regardless of size, into a fixed-size output known as a hash. A key element of the blockchain, the hash function is utilized to guarantee the validity and integrity of data within the system. A cryptographic hash function creates a unique hash for each block on the blockchain. When each block's hash is determined using the hash of the one before it, a chain of blocks is created that cannot be changed without being discovered. This is because any change to the data in a block will lead to the generation of a new hash value, which will then break the chain of hashes and be detectable by all nodes in the network. As a result, the usage of hash functions in blockchain technology offers a safe and immutable method of data storage that guards against unauthorized alterations.

2.1.2 Public Key Cryptography

A vital element in the security of blockchain technology is public key cryptography, which is a fundamental instrument in the field. Public key cryptography encrypts and decrypts messages using a public key and a private key[15]. The public key is made available to everyone who wants to connect with the key owner, while the private key is kept secret and only known by the key owner. Cryptography of public key is used in the context of blockchain to guarantee that only the legitimate owner of a specific digital asset can access it. In a blockchain network, each new transaction is signed by the user using their private key. The transaction is then confirmed to be genuine and approved by the key owner by using their public key to validate the signature. By ensuring that only the legitimate owner of a digital asset can transfer it to someone else, this method ensures the integrity of the transaction and aids in preventing fraudulent behaviors like double-spending. Digital wallets, which enable users to safely store their digital assets and control their transactions in a blockchain network, are also made using public key cryptography.

2.1.3 Digital Signature

In Figure 2, To guarantee the veracity and integrity of transactions, blockchain technology uses cryptography, which is crucially dependent on digital signatures. A mathematical technique known as a digital signature is used to verify the authenticity of a digital communication or document. It entails utilizing a public key infrastructure (PKI) to create a unique digital fingerprint, or hash, of a message or transaction's contents.

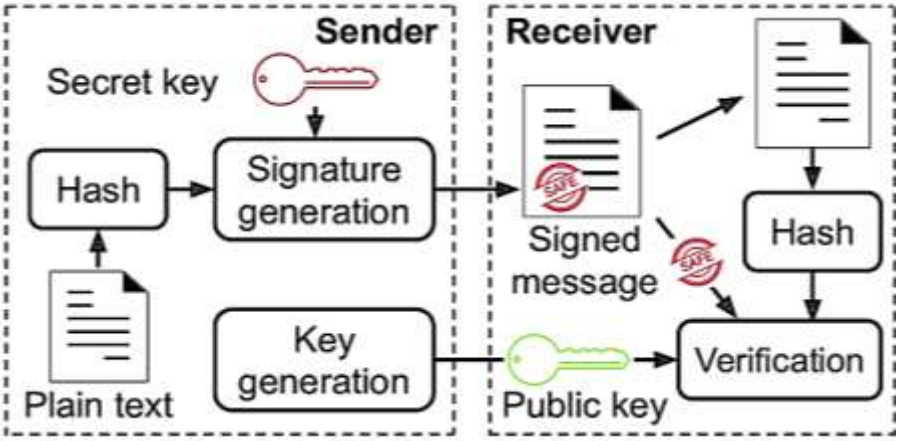

Figure: 2 Digital Signature algorithm[16]

Using the sender's private key, every transaction in blockchain technology is digitally signed. The digital signature is then verified by the receiver using the sender's public key. The receiver can be confident that the transaction hasn't been tampered with and is authentic if the digital signature is valid. Blockchain technology depends on digital signatures to keep the system secure and trustworthy. They give a method for settling disputes, ensuring that transactions are not tampered with, and prohibiting unauthorized access. They are frequently utilized in blockchain-based platforms like Bitcoin, Ethereum, and Ripple and have established themselves as a fundamental part of contemporary cryptographic protocols.

1.4 Public, Private and Permissioned Blockchain

Blockchain technology can be categorized into several types of networks based on its different features which depend on different configurations, network sizes, and consensus methods. Blockchain networks can be differentiated by two dimensions, public or private, defining who is permitted to participate, and permissioned or permission less, defining how participants obtain accessibility to the network.

2.1.4 Public Blockchain

The public blockchain is totally decentralized and not controlled by any one entity. The term "public" suggests that no one will have exclusive access to information but rather that it would be made available to everybody for input during the decision-making process. Since the network is open to the public, creating new blocks is a computationally intensive process that results in high transaction fees. In public or permission less ledgers, users keep a copy of the ledger on their local nodes and use a distributed consensus process to determine the final state of the ledger, regardless of whether or not they are compensated for their participation. Therefore, all public network nodes are of equal significance.

2.1.5 Private Blockchain

The flaws of the public blockchain have led to the emergence of the private blockchain and the exploration by some organizations to be used in business as an alternative to the public blockchain. A private blockchain restricts public access to the blockchain network to participants who have received permission from predetermined administrators, therefore, these blockchains are only partially decentralized. Private blockchains have different requirements compared to public blockchain systems and, therefore, need alternative consensus algorithms and technical trade-offs[17]. A private blockchain which is categorized as a permissioned blockchain is controlled by a single organization where a central authority will decide who can be a node.

2.1.6 Permissioned Blockchain

Emerged as an alternative to the public blockchain, the permissioned blockchain was constructed to tackle the demand for running blockchain technology among a group of recognized and identifiable participants that must be clearly acknowledged by the blockchain network. In a permissioned blockchain, joining the network requires authorization from the network administrator. Also known as private blockchains, the permissioned blockchain also allows for customization to be more effective in maintaining the stability of the data added to the blockchain. As the permissioned blockchain network access is limited which led to the lesser nodes, this network tends to be more efficient allowing for faster transaction processing time.

3. CYBERSECURITY REQUIREMENTS IN BANKING SYSTEMS

Requirements in Banking Systems include the necessary procedures that need to be taken to secure vital financial information, to make sure the systems are reliable, and to make sure that the customers will not feel insecure regarding the existing cyber threats[18]. The requirements are aimed at keeping data confidential and integrity intact and having effective risk management measures to combat threats like phishing, denial of service attacks, insider abuse and malware attacks on bank operations.

3.1 Data Confidentiality and Integrity

Data confidentiality and integrity are fundamental pillars of information security that play a crucial role in safeguarding sensitive and valuable data from unauthorized access, disclosure, or tampering. These concepts are particularly vital in the context of organizations and financial institutions.

Data confidentiality refers to the assurance that information is not disclosed to unauthorized individuals, entities, or systems. It involves protecting data from unauthorized access, ensuring that only authorized personnel can access and use sensitive information. Breaches in confidentiality can lead to identity theft, financial fraud, and erode the trust individuals place in the institution.

Data confidentiality and integrity are interdependent[19]. While confidentiality prevents unauthorized access to sensitive information, integrity ensures that the data accessed is accurate and trustworthy. Achieving a balance between stringent confidentiality measures and allowing authorized personnel access for maintaining data integrity is a complex challenge.

The evolving landscape of cyber threats, including phishing attacks, ransomware, and social engineering, poses significant challenges data confidentiality and integrity. Malicious or unintentional actions by employees within an organization can also pose risks to data security. Some types of cyber threat are shown in Figure 3.

Figure: 3 Schematic of Various Types of Cyber Threats

3.2 Cybersecurity Risk Management

A balanced approach between regulation and operational freedom is essential to ensure strong cybersecurity while maintaining efficiency in financial operations[20][21]. The financial industry faces various cyber-attack vectors, including phishing, Denial of Service (DDoS), ransomware, and insider attacks[22]. These threats pose significant risks to financial institutions and their customers, leading to data breaches, financial losses, and reputational damage.

3.1.1 Phishing Attacks

Phishing, one of the most common forms, manipulates individuals into disclosing sensitive information through deceptive emails that seem to come from trusted sources. The email includes a malicious link that directs the user to a fake website, capturing their login credentials. These attacks are especially effective because they exploit human emotions like fear, curiosity, or the desire to be helpful, making technical defences inadequate without strong employee awareness and training programs.

3.1.2 Denial of Service (DDoS) Attacks

Denial of Service (DDoS) attacks are a pervasive and evolving threat to financial institutions, designed to overwhelm systems with excessive traffic, rendering critical services inaccessible to legitimate users[23]. These attacks flood networks, servers, or applications with massive amounts of data requests, often originating from a distributed network of compromised devices known as botnets.

3.1.3 Insider Attacks

Insider threats in cybersecurity are particularly insidious because they originate from individuals who already possess legitimate access to an organization's systems, such as employees, contractors, or business partners. These threats can be malicious, where an individual intentionally seeks to cause harm, or unintentional, stemming from negligence or lack of awareness.

3.1.4 Malware Threats

Malicious code and malware threats pose a persistent and evolving challenge in the financial industry, exploiting technological vulnerabilities and human factors to infiltrate secure systems[24]. Malware manifests in various forms, such as spyware that covertly monitors user activities, keystroke loggers that capture sensitive information like passwords and financial credentials, and Trojan horses disguised as legitimate software to gain unauthorized access.

4. BLOCKCHAIN-ENABLED CYBERSECURITY IN BANKING

Cybersecurity in Banking dwells on the use of blockchain technology in enhancing the security of the digital financial ecosystem[25]. Blockchain improves the security of transactions by leveraging the decentralization, immutability, and cryptographic principles, which help to facilitate sound fraud detection and prevention, and secure identity management with automated KYC/AML compliance, promoting trust, transparency, and resilience in the current banking environment[26].

4.1 Secure Financial Transactions

The integration of blockchain technology in securing financial transactions reveals notable improvements in security features. Blockchain's inherent characteristics, such as immutability and decentralized ledger technology, provide a robust defense against common cybersecurity threats like data tampering, fraud, and unauthorized access[27]. The security analysis, conducted through various attack simulations and forensic evaluations, affirms the superiority of blockchain-based systems over traditional financial transaction mechanisms.

In the world of financial transactions, blockchain technology is a revolutionary force that has the potential to raise security standards and change the way that financial transactions are carried out. Blockchain is essentially a dispersed, decentralized ledger that uses a computer network to safely and publicly record transactions[28]. Unlike traditional centralized systems, which are controlled by a single entity, blockchain depends on a consensus mechanism to ensure that all participants in the network agree that a transaction is legitimate.

In the realm of money transaction security, blockchain's application extends to various areas. From cross border payments to remittance and supply chain finance blockchain provider transparent and efficient mechanism for verifying the recording transactions. The Decentralized finance (DeFi) platforms are becoming more popular, and they use blockchain technology to provide financial services without the use of middlemen. creating a more inclusive and secure financial ecosystem[29].

4.2 Fraud Detection and Prevention Mechanisms

Blockchain is a decentralized digital ledger that securely, openly, and irrevocably documents transactions. It is made up of cryptographically connected blocks that guarantee data integrity and guard against unwanted changes. Among the main characteristics of blockchain technology are[30]:

- Decentralization: Blockchain runs on a distributed network, lowering the possibility of single points of failure in contrast to traditional banking systems, which depend on centralized databases[31].
- Transparency: Since all parties can see transactions recorded on the blockchain, fraudulent activity is reduced.
- Immutability: Data integrity is ensured by the inability to change or remove a transaction after it has been recorded.
- Smart Contracts: These self-executing, automated contracts lower the danger of fraud by enforcing predetermined rules.

Banking security and transparency are improved by using blockchain technology in fraud detection systems. Figure 4 shows blockchain for fraud detection.

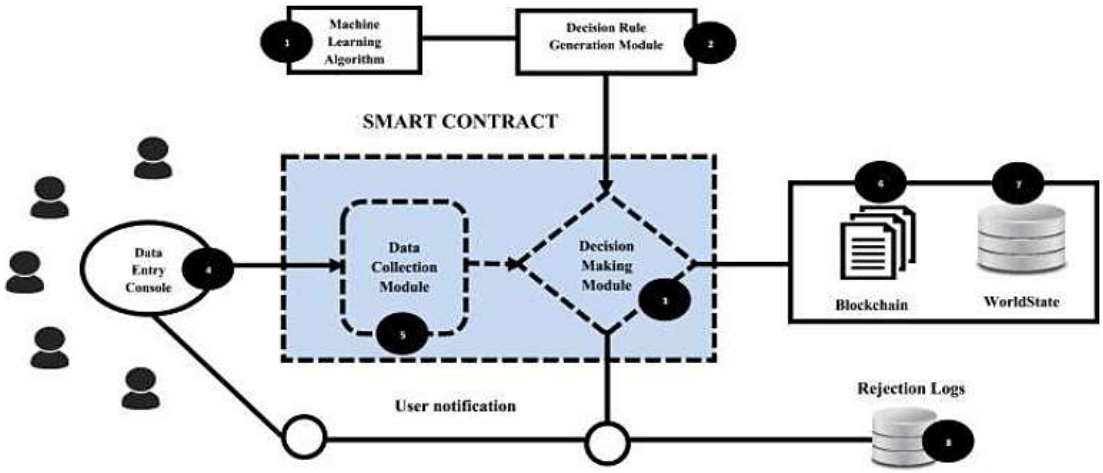

Figure: 4 Blockchain for Fraud Detection

4.3 Blockchain-Based Identity Management and KYC/AML Compliance

Identity verification remains one of the most vulnerable areas of digital banking fraud, often exploited through phishing and synthetic identity creation[32]. Blockchain provides a secure, decentralized framework for identity management, enabling users to control and authenticate their credentials without relying on centralized databases. Digital identities stored on blockchain are encrypted, immutable, and accessible only with user consent, significantly reducing risks of theft or forgery.

In regulatory compliance, blockchain supports Know Your Customer (KYC) and Anti-Money Laundering (AML)requirements by creating immutable records of customer verification and transaction histories. Once verified, customer credentials can be reused across multiple financial institutions without redundant processes, lowering costs while maintaining regulatory integrity[33].

Figure 5 presents the workflow of blockchain-enabled fraud prevention in a digital banking transaction cycle, illustrating how real-time verification, smart contracts, and identity management converge to create multilayered defences. The figure demonstrates how data validation, risk scoring, and compliance reporting integrate seamlessly into a single framework. By embedding compliance into blockchain protocols, banks can automate detection of suspicious activity, improve reporting accuracy, and reduce penalties for regulatory breaches[34]. This capability strengthens both institutional resilience and consumer trust in financial systems.

Figure: 5 Blockchain-enabled Fraud prevention in Digital Banking

5. LITERATURE REVIEW

The section is an overview of the recent research on cybersecurity in the banking industry, especially related to cyber threat analysis, blockchain-related security, and AI-driven protection systems. The works under consideration focus on the comprehension of emerging threats, the enhancement of the security of transactions, and the enhancement of digital banking systems, and discuss the issues concerning scalability, compliance with the regulations, and their proper implementation.

Tonnonlah et al. (2025) analyzes the cybersecurity threats by collecting information from customers through a survey, cybersecurity experts and also banking professionals. The survey explores the effectiveness of security measures and awareness among stakeholders, the goal is to comprehend the most pressing security concerns, to evaluate how the current protections are working and identify lacks or problems that needs be solved. the findings concentrate on emerging security challenges and offer solutions for strengthening

security in IoT-enabled banking industry, to be prepare ahead for these threats with advanced security protocols to help the financial organizations and customers from cyber threats[35].

Roy et al. (2025) explores how blockchain technology might improve cyber-security and operational effectiveness in the banking industry. The decentralized and immutable characteristics of blockchain technology can safeguard transactions, lower fraud, and increase transparency, as demonstrated by a Hyperledger Fabric prototype. When compared to conventional systems, the results demonstrate notable gains in transaction speed, cost-effectiveness, and security. Issues like scalability and regulatory compliance are brought to light, highlighting the necessity for more study. Blockchain is regarded as a game-changing tool for rethinking banking trust and safeguarding financial ecosystems[36].

Paul and Kulkarni (2024) investigates the application of blockchain in secure banking, focusing on the integration of tools such as Meta Mask and Ganache for the implementation of the system and machine learning algorithms to detect the illegaltransactions. Through a comprehensive literature review, methodology, implementation strategies, case-studies, challenges, and future prospects. The paper provides a thorough analysis of blockchain's role in secure online banking system with the help of machine learning. Key findings indicate that blockchain can significantly mitigate fraud, streamline operations, and enhance data integrity, though challenges such as scalability and regulatory compliance must be addressed in the banking systems with the help of machine learning classifying algorithms[37].

Nakonechnyi et al. (2024) aims to examine the impact of blockchain implementation in the banking system, focusing on its ability to enhance the protection of online banking operations. It aims to elucidate the advantages and disadvantages of this platform in the banking industry, with a particular emphasis on its technical functionalities and consensus algorithms. The models and block architecture, the study analyses the technical functionalities of blockchain technology, drawing comparisons with traditional banking systems. The research also explores the application of security, verification, and decentralisation features to prevent fraudulent activities and ensure transaction integrity, mainly focusing on the banking landscape in India. Initial findings indicate that blockchain technology holds promising prospects for improving banking efficiency, with its structures efficiently tracking transactions and preventing unauthorised alterations[38].

Darem et al.(2023) provide a comprehensive analysis of cyber threats in the banking and financial sectors, including identifying common threats, their nature and character to help in classification. One of the significant contributions of this research paper is to classify cyber threats to the banking and financial sectors based on their severity and technicality. This classification helps to identify the appropriate countermeasures required to mitigate the risks of each type of threat. Furthermore, the paper explores the technical, non-technical, organizational countermeasures and the legal and regulatory measures used to protect financial transactions from cyber threats. This research work delves into the challenges and limitations of cyber threat classifications, focusing specifically on those confronting the banking and financial sector in their pursuit of robust cybersecurity[39].

Dasgupta et al. (2023) explores the role of AI in identifying threats in digital banking and highlights the benefits of using AI-powered cybersecurity to support business efficiency. The study also aims to raise awareness about the need to overcome the fear of experimenting with new technologies and to show how examples of Malta's risk management study drawing on the experiences of businesses that have implemented AI-powered cybersecurity systems in Malta, highlighting the success of such systems in safeguarding business operations. The study also examines the challenges of implementing AI-powered cybersecurity and offers recommendations for overcoming these challenges. The findings of this study contribute to the body of knowledge on the role of AI in cybersecurity and provide insights for businesses looking to implement AI-powered cybersecurity systems[40].

Table I shows the recent findings in the domain of cybersecurity in banking, where the recent approaches include cyber threat analysis, blockchain-based security measures, and AI-controlled protection mechanisms. Although the reviewed works are highly promising in terms of enhancing transaction security, prevention of fraud, and risk management, numerous studies show weaknesses associated with scalability, compliance to regulations, and large-scale practical implementation.

TABLE I. SUMMARY OF RELATED WORKS ON BLOCKCHAIN-ENABLED CYBERSECURITY IN THE BANKING SECTOR

Author(s)	Focus Area	Methodology	Key Contributions & Findings	Limitations / Future Work
Tonnonlah et al. (2025)	Cybersecurity threats in IoT-enabled banking	Surveys of customers, cybersecurity experts, and banking professionals	Assessed stakeholder awareness and effectiveness of existing security measures; identified critical and emerging cybersecurity challenges in IoT-based banking; proposed advanced security protocols to enhance protection for financial institutions and customers.	Relies on perception-based survey data; future work may include real-time threat detection systems and empirical validation using operational banking data.
Roy et al. (2025)	Blockchain-based cybersecurity and operational efficiency in banking	Blockchain technology, Hyperledger Fabric prototype	Demonstrated that decentralized and immutable blockchain features improve transaction security, reduce fraud, enhance transparency, and increase transaction speed and cost efficiency compared to conventional systems.	Scalability and regulatory compliance remain challenges; further studies are required for large-scale and cross-border banking deployment.

Paul and Kulkarni (2024)	Secure online banking using blockchain and machine learning	Blockchain (MetaMask, Ganache), machine learning-based fraud detection	Provided a comprehensive analysis of blockchain-enabled secure banking integrated with ML classifiers; showed improvements in fraud mitigation, data integrity, and operational efficiency.	Scalability, regulatory constraints, and optimization of ML classification models require further investigation.
Nakonechnyi et al. (2024)	Impact of blockchain on online banking security	Blockchain architecture analysis, consensus mechanisms, comparative models	Examined blockchain's technical functionalities, including decentralization, verification, and consensus algorithms; demonstrated its potential to prevent fraud and ensure transaction integrity, with emphasis on the Indian banking context.	Limited empirical validation; future research may focus on performance benchmarking and real-world banking implementations.
Darem et al. (2023)	Cyber threat classification in banking and financial sectors	Threat taxonomy, severity-based and technical classification, literature analysis	Proposed a structured classification of cyber threats based on severity and technical complexity; analyzed technical, organizational, legal, and regulatory countermeasures for protecting financial transactions.	Static threat classifications may struggle with rapidly evolving cyber risks; future work may explore adaptive and AI-driven threat modeling approaches.
Dasgupta et al. (2023)	AI-powered cybersecurity in digital banking	AI-based threat detection, case studies, risk management analysis (Malta)	Highlighted the effectiveness of AI-driven cybersecurity solutions in detecting threats and improving business efficiency; emphasized organizational readiness and adoption of AI security systems.	Challenges include trust, skill gaps, cost, and implementation complexity; future work may focus on explainable AI and broader geographic validation.

6. CONCLUSION AND FUTURE WORK

The growing use of online banking services has posed more cybersecurity risks, and this has brought the need to implement strong and resilient security systems to ensure that confidential financial information is not compromised. The paper has discussed blockchain-based cybersecurity as a potential way to enhance the security of the contemporary banking system. The paper has illuminated the potential of blockchain technology to enhance the security of the banking sector through decentralization, immutability and cryptographic methods, which can help to reduce the risk of data tampering, fraud, identity theft and unauthorized access. It has been shown in the analysis that blockchain will increase safe financial transactions, better fraud detection and prevention, and reliable identity management along with built-in KYC and AML compliance. Although blockchain has notable benefits, its implementation in the banking sector is limited by issues associated with scalability, regulatory conformity, compatibility with standing systems and complexity of operations. On the whole, the results suggest that blockchain can be regarded as an additional cybersecurity control instead of alternative to conventional security solutions, which can be used to ensure the creation of transparent, reliable, and trustful digital banking ecosystems. Future studies can take into consideration the large-scale application of blockchain-based cybersecurity models in the banking setting. Research should also be done on optimizing scalability, aligning regulation with different jurisdictions, and smooth integration with AI driven security systems. Furthermore, it would be more informative to compare performance and cost-effectiveness, and user acceptance of live banking applications to learn more about their practical implementation.

REFERENCES

[1] F. Jimmy, "Cybersecurity Threats and Vulnerabilities in Online Banking Systems," *Int. J. Sci. Res. Manag.*, vol. 12, no. 10, pp. 1631–1646, Oct. 2024, doi: 10.18535/ijsrm/v12i10.ec10.

[2] G. Sarraf and V. Pal, "Autonomous Threat Detection and Response in Cloud Security: A Comprehensive Survey of AI-Driven Strategies," *Int. J. Emerg. Res. Eng. Technol.*, vol. 6, no. 4, 2025, doi: 10.63282/3050-922X.IJERET-V6I4P114.

[3] T. Shah, "Leadership in digital transformation: Enhancing customer value through AI-driven innovation in financial services marketing," *Int. J. Sci. Res. Arch.*, vol. 15, no. 3, pp. 618–627, Jun. 2025, doi: 10.30574/ijsra.2025.15.3.1767.

[4] I. P. Mandliya, "A Study On Cyber Security Affecting Online Banking And Online Transaction," 2023.

[5] S. Thangavel, S. Srinivasan, S. B. V. Naga, and K. Narukulla, "Distributed Machine Learning for Big Data Analytics: Challenges, Architectures, and Optimizations," *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 4, no. 3, pp. 18–30, Oct. 2023, doi: 10.63282/3050-9262.IJAIDSML-V4I3P103.

[6] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[7] K. S. Hebbar, "Optimizing Distributed Transactions in Banking APIs: Saga Pattern vs. Two-Phase Commit (2PC)," *Am. J. Eng. Technol.*, vol. 7, no. 06, pp. 157–169, 2025, doi: 10.37547/tajet/Volume07Issue06-18.

[8] V. Verma, "Deep Learning-Based Fraud Detection in Financial Transactions : A Case Study Using Real-Time Data Streams," vol. 3, no. 4, pp. 149–157, 2023, doi: 10.56472/25832646/JETA-V3I8P117.

[9] P. Ogeti, N. S. Fadnavis, G. B. Patil, U. K. Padyana, and H. P. Rai, "Blockchain Technology for Secure and Transparent

Financial Transactions," *Eur. Econ. Lett.*, vol. 12, no. 2, p. 9, 2022.

[10] P. Gupta, S. Kashiramka, and S. Barman, "A Practical Guide for Ethical AI Product Development," in *2024 IEEE 11th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/UPCON62832.2024.10983504.

[11] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, "Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality," in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, IEEE, 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.

[12] S. Yadav, "Role of Blockchain Technology in Enhancing Cybersecurity," *Int. J. LAW Manag. Humanit.*, vol. 8, no. 3, p. 10, 2025.

[13] M. Birje, R. H. Goudar, R. C. M, and M. T. Tapale, "Blockchain Technology Review: Consensus Mechanisms and Applications," *Int. J. Eng. Trends Technol.*, vol. 71, no. 5, pp. 27–39, May 2023, doi: 10.14445/22315381/IJETT-V71I5P204.

[14] R. Soltani, M. Zaman, R. Joshi, and S. Sampalli, "Distributed Ledger Technologies and Their Applications: A Review," *Appl. Sci.*, vol. 12, no. 15, p. 7898, Aug. 2022, doi: 10.3390/app12157898.

[15] S. Ahmad, S. K. Arya, S. Gupta, P. Singh, and S. K. Dwivedi, "Study of Cryptographic Techniques Adopted in Blockchain," in *2023 4th International Conference on Intelligent Engineering and Management (ICIEM)*, IEEE, May 2023, pp. 1–6. doi: 10.1109/ICIEM59379.2023.10166591.

[16] B. Kieu-Do-Nguyen, C. Pham-Quoc, N.-T. Tran, C.-K. Pham, and T.-T. Hoang, "Low-Cost Area-Efficient FPGA-Based Multi-Functional ECDSA/EdDSA," *Cryptography*, vol. 6, no. 2, p. 25, May 2022, doi: 10.3390/cryptography6020025.

[17] N. M. Nasir, S. Hassan, and K. Mohd Zaini, "Securing Permissioned Blockchain-Based Systems: An Analysis on the Significance of Consensus Mechanisms," *IEEE Access*, vol. 12, pp. 138211–138238, 2024, doi: 10.1109/ACCESS.2024.3465869.

[18] A. R. Bilipelli, "Forecasting the Evolution of Cyber Attacks in FinTech Using Transformer-Based Time Series Models," *Int. J. Res. Anal. Rev.*, vol. 10, no. 3, pp. 383–389, 2023.

[19] A. Anyanwu, T. Olorunsogo, T. O. Abrahams, and O. J. Akindote, "ata Confidentiality And Integrity: A Review Of Accounting And Cybersecurity Controls In Superannuation Organizations," *Comput. Sci. IT Res. J.*, vol. 5, no. 1, pp. 237–253, Jan. 2024, doi: 10.51594/csitrj.v5i1.735.

[20] S. K. Chintagunta and S. Amrale, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *Tech. Int. J. Eng. Res.*, vol. 9, no. 10, pp. 49–55, 2022, doi: 10.56975/tijer.v9i10.159996.

[21] N. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity : A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, pp. 520–528, 2025, doi: 10.48175/IJARSCT-25168.

[22] E. McCoy, "Cybersecurity Regulations and Risk Management in the Financial Sector: A Comparative Analysis," *Law, Econ. Soc.*, vol. 1, no. 1, p. p115, 2025, doi: 10.30560/les.v1n1p115.

[23] A. Parupalli, "Business Intelligence in ERP ML-Based Comparative Study for Financial Forecasting," *ESP Int. J. Commun. Eng. Electron. Technol.*, vol. 2, no. 4, pp. 17–26, 2024, doi: 10.56472/25839217/IJCEET-V2I4P103.

[24] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, 2025.

[25] D. Patel, "Enhancing Banking Security: A Blockchain and Machine Learning- Based Fraud Prevention Model," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 576–583, 2023, doi: 10.14741/ijcet/v.13.6.10.

[26] S. B. Karri, S. Gawali, S. Rayankula, and P. Vankadara, "AI Chatbots in Banking: Transforming Customer Service and Operational Efficiency," in *Advancements in Smart Innovations, Intelligent Systems, and Technologies*, 2025, pp. 61–81. doi: 10.3233/FAIA251498.

[27] A. Roy and S. S. Tinny, "Cybersecurity and Blockchain for Secure Financial Transactions: Evaluating, Implementing, and Mitigating Risks of Digital Payments," *Int. J. Appl. Nat. Sci.*, vol. 1, no. 2, pp. 38–48, Aug. 2024, doi: 10.61424/ijans.v1i2.95.

[28] H. Patel, O. Patil, M. Makandar, and R. Patel, "Enhancing Money Transaction Security Through Blockchain Technology : A Comprehensive review and Analysis," 2024. doi: 10.2139/ssrn.4963437.

[29] S. R. Kurakula, "Designing Enterprise Systems for the Future of Financial Services: The Intersection of AI, Cloud-Native Microservices, and Intelligent Data Processing," *Eur. J. Comput. Sci. Inf. Technol.*, vol. 13, no. 20, pp. 91–103, 2025.

[30] M. S. Parvez and M. R. Khan, "The Role of Blockchain in Banking Fraud Detection: Enhancing Security and Transparency," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 2, pp. 386–394, Apr. 2025, doi: 10.32996/jcsts.2025.7.2.40.

[31] H. P. Kapadia, "CDN Strategies for Secure and Fast Banking Services," *Int. J. Curr. Sci.*, vol. 12, no. 4, pp. 863–869, 2022.

[32] S. J. Wawge, "A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3345–3352, May 2025, doi: 10.38124/ijisrt/25apr1813.

[33] R. Palwe, "Adaptive human: AI decision support for high-stakes financial advice," *Int. J. Comput. Artif. Intell.*, vol. 6, no. 2, pp. 385–392, Jul. 2025, doi: 10.33545/27076571.2025.v6.i2e.226.

[34] O. M. Eseoghnene, "Applying Blockchain-Based Fraud Prevention Mechanisms for Securing Digital Banking Transactions and Strengthening Customer Trust in Financial Institutions Worldwide," *Int. J. Res. Publ. Rev.*, vol. 6, no. 9, pp. 351–367, Sep. 2025, doi: 10.55248/gengpi.6.0925.3334.

[35] D. Tonnonlah, S. F. Juma, S. Yandokoye, and A. Pandey, “Cybersecurity Threats in IoT-Enabled Banking: Survey & Solutions,” in *2025 International Conference on Intelligent and Secure Engineering Solutions (CISES)*, IEEE, Aug. 2025, pp. 610–619. doi: 10.1109/CISES66934.2025.11265429.

[36] T. Roy, M. I. Alam, A. Turag, S. R. Chowdhury, and A. Kafi, “Securing Blockchain in Banking: Cyber Threat Mitigation,” in *2025 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, IEEE, Feb. 2025, pp. 1–4. doi: 10.1109/ECCE64574.2025.11013217.

[37] V. Paul and P. Kulkarni, “Integration of Blockchain Technology and Machine Learning in Online Secure Banking System,” in *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, IEEE, Nov. 2024, pp. 1–4. doi: 10.1109/CSITSS64042.2024.10816977.

[38] V. Nakonechnyi, S. Toliupa, V. Saiko, V. Lutsenko, G. S. N. Ghno, and A. K. Hussain, “Blockchain Implementation in the Protection System of Banking System During Online Banking Operations,” in *2024 35th Conference of Open Innovations Association (FRUCT)*, IEEE, Apr. 2024, pp. 492–500. doi: 10.23919/FRUCT61870.2024.10516404.

[39] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi, and S. A. Ebad, “Cyber Threats Classifications and Countermeasures in Banking and Financial Sector,” *IEEE Access*, vol. 11, pp. 125138–125158, 2023, doi: 10.1109/ACCESS.2023.3327016.

[40] S. Dasgupta, B. V. Yelikar, Ramnarayan, S. Naredla, R. K. Ibrahim, and M. B. Alazzam, “AI-Powered Cybersecurity: Identifying Threats in Digital Banking,” in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, IEEE, May 2023, pp. 2614–2619. doi: 10.1109/ICACITE57410.2023.10182479.

