International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 10, October 2026)

Cyber - Integrated Anti Money Laundering System for Pre - Transaction Fraud Prevention

Chaithra K[1], Kavyashree G Bhat[2], Monisha PS[3], Rashmi V Shetty[4], Dr. Kavita K Patil[5]
[1]*Department of ISE, Global Academy of Technology, Bengaluru, India*
Associate Professor, ISE, Global Academy of Technology, Bengaluru, India

***Abstract*— The rapid growth of online banking, mobile payments, and digital financial services has improved transaction speed and accessibility but has also increased risks such as phishing, fraud, unauthorized account access, identity theft, and money laundering, making financial security a major concern for banks and regulators [2][4][8].Current Anti-Money Laundering (AML) systems mainly detect suspicious transactions after processing, while cybersecurity solutions focus on network security and authentication rather than verifying transactions before completion [9][10][11].This survey reviews AI, Machine Learning (ML), behavior analytics, blockchain, anomaly detection, and Zero Trust frameworks for fraud detection and cybersecurity in banking [1][3][5][6][14][20]. AI identifies suspicious transaction patterns and user behavior, while blockchain improves data integrity and transparency. However, existing approaches are not fully integrated and address only specific security aspects [9][10][12][13]. This survey highlights current research, limitations, and future directions, emphasizing the need for a unified cyber-integrated AML framework for secure pre-transaction fraud detection and stronger financial security [1][5][7][9][12][20].**

***Keywords*— Artificial Intelligence, Anti-Money Laundering, Behavioral Analytics, Blockchain, Cybersecurity, Fraud Detection, Machine Learning.**

I. Introduction

The financial sector is undergoing a massive transformation with the advent of digital banking, internet banking, mobile payment applications and financial technology, which makes banking more efficient, accessible, and customer-centric [2][6][8][20]. These developments have been welcomed by millions of investors and bankers. But this surge in digital banking has created new vulnerabilities for criminals to attack, including through a combination of phishing, identity theft, malware and ransomware attacks, account takeover, insider threats, and money laundering attacks [2][4][6][8][17].

The financial institutions use traditional anti-money laundering (AML) systems to find out fraudulent transactions and meet regulatory needs. [16][17][18] [19].

Those systems mostly carry out analysis on completed transactions based on pre-defined rules, thresholds and transaction history to detect fraud. Although these systems are useful for regulatory purposes, they are only able to identify suspicious transactions after the transaction is finished so they are not capable of stopping financial loss in real time [9][10][11][12].

In the same manner, the current cyber security structures examine utilization subtleties, IP addresses, network traffic and access control to recognize and determine cyber dangers and illegitimate access [2][3][6][15]. These systems are usually not connected to AML systems nor to the other AML systems, and do not help to fight financial fraud in a coordinated manner [4][9][19][20].

II. Literature Review

The literature survey gives comprehensive information on existing studies on Artificial Intelligence (AI), Machine Learning (ML), cyber security, Anti-Money Laundering (AML), blockchain technology, behavioral analysis, anomaly detection, banking fraud detection. The study of available literature helps in understanding the methods used, the important contributions of various authors, merits, and demerits and the research gaps. This study serves as the background for developing our Cyber-Integrated AntiMoney Laundering system for the purpose of pretransaction fraud prevention. It combines the use of cyber security controls with smart transaction processing method For the prevention of fraud[1][3][5][7][9][14].

Digitalization and advancement of on the web installment frameworks; versatile portable internet banking applications has expanded credit and debit. As of late this development has prompt a lot of cyber aggressions on the frameworks of managing an account institutions, financial associations, and payment platforms [2][4][6][8]. Bank cyber criminals make use of deceptive tactics, for example, phishing schemes, individual data robbery, hacking of bank accounts, and installing malicious software applications in a way to loot financial institutions and commit money laundering. These are major forms of threats directed on financial associations.

In response to this crisis, researchers develop strategies applying several mechanisms and methods including Artificial Intelligence (AI), Machine Learning (ML), blockchain, behavioral examination, inconsistency determination and cyber securities frameworks (e.g. Intrusion Detection System, Intrusion prevention system) towards controlling the issue [1][3][5][6][14][18]. Artificial Intelligence and Machine Learning techniques are among the core mechanisms when identifying fraud dealings on the records by investigating conduct of customer transaction history and unusual purchase activities. Intelligent machine learns on-goingly as they get information history.

These methods have been far better over traditional procedures depending upon the principles to discover the fake records [3][5][6][7][12].Various protection contraption in the cybersecurity arena namely multifactor verifications, behavioral examination systems (BBS), record and email Encryption technology, and the usage of the security frameworks on the premise of the principle of zero believe will be utilized by financial institutions against unauthorized digital intrusions. A protected framework with the use of intrusion Prevention Device/Detection FrameWork could preclude or deter unauthorized access. Nevertheless, current investigations are largely focused on solitary methods. So we investigate current research in the context of our proposed frame work and highlight the weakness for the prevention of transactions against malicious attacks in the sphere of fraud activities in [9][10][11][13].

1. FRAUD-X: An Integrated AI, Blockchain, and Cybersecurity Framework with Early Warning Systems for Mitigating Online Financial Fraud The authors Bekim Fetaji et al. In [1] propose the FRAUD-X framework to prevent online financial fraud through the combination of AI, blockchain, and cybersecurity. It includes a component to integrate AI based anomaly detection, blockchain's tamper proof ledger and early warning systems that identifies suspicious online transaction in real time. While AI constantly monitors and analyzes transaction behavior, blockchain maintains transparent, secure ledger of each transaction. The proposed solution contributes to greater accuracy on detecting fraud and to improved data authenticity and faster warnings to customers and financial services. The drawbacks include the increase in complexity and computational cost of combining AI and blockchain and the challenge this poses for implementing them in small financial organizations.

2. Cybersecurity Strategies for Safeguarding Customer Data and Preventing Financial Fraud in the United States Financial Sectors In their paper [2], Efijemue Oghenekome Paul et al. Focused on the critical necessity for efficient cybersecurity strategies that protect customer data and prevent financial fraud.

Through strategies like encryption, multi-factor authentication, Identity management, continuous system monitoring and employees training and education, banking security becomes stronger. Furthermore, the researchers claim that the adoption of AI and Machine Learning in cybersecurity architectures further improve detection time of cyber threats while reducing unauthorized access to financial systems. As effective as this may be for protecting sensitive data, it lacks a critical point of focus, the integration of Anti-Money Laundering transaction analysis as a form of enhancing financial fraud detection.

3. The Role of Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance Layla Abdel-Rahman Aziz and Yuli Andriansyah in [3] provided an overview of AI use for fraud detection, risk management and compliance. They explained how AI strategies like deep learning, NLP, predictive analytics, behavioral biometrics and graph analysis help banks identify fraudulent acts more than rule based systems. AI can also enhance KYC verification process and automate the regulatory compliance. However, they argued that the efficiency of AI is heavily reliant on the quality and size of data, continuous retraining of models and appropriate implementation.

4. Cyber Security and Internet Banking: Issues and Preventive Measures In their study, Leandre Gomes, Abhinav Deshmukh, and Nilesh Anute analyzed major security issues related to internet banking and suggested preventive strategies. The growing use of internet banking also brings increased rate of cyber threats and financial fraud such as phishing, malware attacks, hacking, and identity theft. For this, security measures like sound authentication systems, encryption, regular updating of software and systems, employees and customers education and awareness, and improved security policies are proposed to make banking platforms more secured. The downside to these security solutions is that they only consider safeguarding the banking platform rather than integrating behavioral analytics or AI that detect frauds in real-time.

5. AI-Driven Fraud Detection in Banking: A Systematic Review of Data Science Approaches to Enhancing Cybersecurity Olawale Olowu et al. [5] proposed a systematic review on AI and data science used for fraud detection. They assessed the efficiency of algorithms like ML, DL and real time monitoring on the task of detecting fraudulent transactions and provided evidence that AI systems are better than conventional rule based systems on terms of accuracy and lower false positive rates.

They found that the application of integrated supervised and unsupervised learning is effective in detecting emerging trends in fraud and that massive data, continuous training and high performance computational resources are necessary for AI to perform effectively.

6. AI-Driven Cybersecurity in Online Banking: Enhancing Fraud Detection and Risk Mitigation Kshitij Shukla, Mohd. Sajid, and Akil Hussain [6] focused on an AI driven cybersecurity framework aimed at improving fraud detection and risk mitigation in online banking platforms. Their article states that AI and ML are essential to secure online banking by using them to analyze behavior, predict risks, and automatically address emerging threats. AI powered solutions constantly monitor transactions and interactions to detect unusual behavior, leading to the reduction of false positive rate unlike conventional security systems. Despite its efficiency, they listed few challenges such as AI biases, data privacy, adversarial attacks and suggested the use of explainable AI and adherence to regulations. Just like other researchers, they reiterated the need for continued training and advanced infrastructure to maximize the framework's utility.

7.AI-Powered Financial Crime Prevention with Cybersecurity, IT, and Data Science in Modern Banking .The work done by Abraham Okandeji Omokanye et al. [7] involved a wide review of AI methods applied to financial crime prevention by combining AI, cybersecurity, Information Technology and Data Science. The application of machine learning based AI approaches in real-time systems proved to be very efficient and reliable than rule based methods, helping to effectively reduce false positive rate, and at the same time enhancing security controls while ensuring overall operational effectiveness. However, the challenges of data privacy, the cost of system integration, as well as the complex regulatory requirements are among the obstacles to efficient implementation.

8. Cybersecurity Risks in Online Banking: A Detailed Review and Preventive Strategies Application Adedoyin Tolulope Oyewole et al. [8] presented a detailed analysis of online banking cyber threats and their prevention. They elaborated on the fact that cyber threats like malware, phishing, identity theft and insider attacks increase with the continuous demand for online banking services and that the integration of advanced strategies like Artificial Intelligence, Big Data analytics, risk assessment and public awareness program can strengthen banking security. The authors concluded that integrated strategies is very necessary to assure the clients that their data is well protected, hence rebuilding trust.

9. An Integrated Cybersecurity and Anti-Money Laundering Governance Framework for Financial Crime Prevention Oladapo Fadayomi et al. [9] put forth an integrated framework that combines Cybersecurity and Anti-Money Laundering (AML) for effective financial crime prevention. The framework emphasizes an organization-wide governance, the integration of technology, processes, and human knowledge as a comprehensive security system where transaction monitoring, intelligent threat detection, and compliance mechanisms are put in place to increase the prevention of cyber-enabled financial crimes and reinforce institutional security. While the study presents governance and policy integration, it barely covers intelligent detection techniques using AI.

10.Enhancing Anti-Money Laundering and CounterTerrorist Financing Strategies through Cybersecurity and Compliance Measures Integrated In this paper, the authors emphasized the benefits of linking cybersecurity methods with AML and CTF compliance. Continuous monitoring, securely sharing information, assessments and regulatory coordination help banks to track suspicious transactions more effectively while reinforcing their own safety. The conclusions that combining both cyber controls and AML procedures creates a robust defense against financial fraud while enhancing governance are drawn. Despite the benefits of the combined procedures, there is minimal focus on AI and real-time behavioral analysis.

11. AML compliance Under Pressure: Between National Security and Financial Inclusion: Oladapo Olatinsu discussed the difficultiesin balancing the adherence to stringent anti-money laundering regulations and financial inclusion. According to the research paper, although robust AML compliance is paramount in preventing money laundering and terrorist financing, overly strict regulatory measures may limit real consumers' accessibility to the financial system. To enhance security and client accessibility, the author suggested a risk-based compliance approach powered by digital identification and advanced monitoring systems. However, the study largely covers policy and regulatory concerns rather than utilizing an intelligent AI-based fraud detection strategy [11].

12. Enhancing Financial Institution Security with AIPowered AML, Fraud Detection and Cyber Risk Management: Haris Ghulam and Nadia Rahman put forward an AI-enhanced framework that encompasses AntiMoney Laundering (AML), fraud detection and cyber risk management to enhance the security of digital finance.

The study showed how ai based showed how AI-based machine learning, predictive analysis and real-time monitoring assist in identifying suspicious transactions efficiently by providing a significant reduction in the number of false positives. The researchers further emphasized the role of AI in automatic report generation to the regulators and risk assessment for customers as well as in the identification of cyber threats. The integration allows for increase in operational efficiency and bank security, but it is important to consider data privacy concerns, ethical issues, and compliance regulations [12].

13. Mitigating Cyber Risk in Financial Institutions: Integration of AI-powered AML, FinTech Innovation and Seamless Financial Services: Naseem Irfan and Nadia Rahman proposed a framework for lessening cyber threats in financial institutions that combines artificial intelligence, innovative FinTech solutions and AntiMoney Laundering techniques. The paper explained how Alpowered monitoring of transactions, use of blockchain, biometric authentication and automated Know Your Customer (KYC) verification help improve the detection of fraud and regulatory compliance significantly. The authors provided information about how the framework offers advanced capabilities for financial institutions to proactively detect fraudulent activities while ensuring secure and seamless financial transactions in the digital environment. However, it also requires continuous system maintenance, high upfront investment, and policy and regulatory challenges [13].

14. Inter-Role of Cybersecurity, AI, and Blockchain in Preventing Money Laundering and Terrorism Financing: The paper explains the combined use of artificial intelligence, blockchain, and cybersecurity to improve Anti-Money Laundering (AML) and counter-terrorism financing (CTF) systems. The authors explained that AIhelps in intelligent fraud detection while blockchain assures secure and tamper-proof transactions and cybersecurity ensures that sensitive data and systems cannot be accessed by authorized parties. Such integration of these technologies further enhanced the monitoring of transactions, compliance with regulations, and transparency of finances. However, it should be notedthat building an AI-blockchain integrated framework demands investment, technology specialists and updated system infrastructure [14].

15. Fraud Detection: A Systematic Literature Review of GraphBased Anomaly Detection Approaches: A study by Tahereh Pourhabibi, Kok-Leong Ong, Booi H. Kam and Yee Ling Boo offered a systematic analysis of graph based anomaly detection methodologies that are employed in the context of financial fraud detection.

As argued in the paper, the structure and features of graph-based models facilitate the accurate detection of fraudulent patterns, which often leverage covert relationships among entities, such as clients, account numbers and their financial transactions. By offering a superior visualization of malicious connections compared to conventional methods and thereby ensuring improved fraud detection outcomes, the use of graph analytics presents the drawback of requiring massive amounts of financial transaction data, considerable computational resources and advanced graph processing algorithms [15].

16. Detecting Insider Threats in Banking Utilizing AI-Based Anomaly Detection with a Data Science Approach to Cybersecurity: Ajayi Akintayo Micheal and co. Described an AI-based anomaly detection model for identifying insider threats in the banking sector. The research is founded upon the principle that it is feasible to detect abnormal behavior of a user, the unauthorized access that an insider may attempt to leverage and also mitigate the security risks as such by conducting constant monitoring of employee activity while using the tools of machine learning, User Entity Behavior Analytics (UEBA) and Behavioral analytics [16]. Data privacy, constant learning system and periodic updating of the model were identified as shortcomings that need careful consideration.

17. Advancements in Cybersecurity Strategies for Financial Institutions to Address E-Channel Fraud in the Digital Era: This article from Anne Ajiri Alex-Omiogbemi and colleagues, reviews emerging cybersecurity techniques that could successfully be deployed to address the increasing number of fraudulent transactions through the channels of e-services in banks. The researchers suggested the implementation of anti-phishing, anti-malware, counteraccount takeovers, behavioral analytics, AI, blockchain, real-time transaction monitoring and biometrics to fortify the security of banks and customer service. As noted, the integration of the technologies above with organizational learning programs helps in reducing echannels fraud and also improves customer loyalty. One drawback the study noted was the narrow scope in which cyber-security was focused, without including anti-money laundering (AML) transaction analysis [17].

18. Defending Against Fraud: cyber Fraud Detection and Prevention techniques: The paper given by Lekgau, Mabitsela M. And Masinga J. Matome discusses up-to-date technologies and methodologies that can be used for the prevention and detection of financial fraud in the banking sector.

The papers provided the application of machine and deep learning, threat intelligence and behavioral analysis for the effective identification of fraudulent practices, reporting that although such techniques improve on what rule-based systems can offer by significantly increasing accuracy and drastically reducing the number of false alarms, they require large data sets, processing power and regular system updates [18].

19. Statistical Analysis of Cyber Risk Exposure and Fraud Detection in Cloud-Based Banking Ecosystems: In his paper, Md. Nahid Hossain developed a statistical framework that can be used for determining risk exposure and detecting fraud in banking organizations that adopt the cloudbased paradigm. The research explains how to enhance banking systems against cyber threats through measures such as, use of statistics in analysis and modeling of risk factors, risk assessment using cloud security best practices, analysis of financial risk, and so on. Such analytical framework helps the organizations know where they are vulnerable so that security measures can be planned and implemented accordingly; but it fails to offer intelligent realtime fraud detection approaches [19].

20. Zero Trust Cybersecurity: Critical Success Factors and a Maturity Assessment Framework: William Yeoh and colleagues provided a framework named Zero Trust Cybersecurity in order to enhance information security within an organization. The paper argues that by implementing Zero Trust Architecture, all users, devices and applications are constantly verified before a user can access them. This ensures that information access remains only to unauthorized personnel thereby enabling the organization to mitigate insider threats and unauthorized usage of sensitive information. The authors also introduced a maturity assessment plan that organizations can use to determine their effectiveness when adopting Zero Trust measures; the only drawback that can be highlighted is the high investment required for large organizations to implement such security measures successfully, alongside continuous monitoring processes and effective management strategies [20].

III. Identification Of Research Gap

The literature review shows that there are important advancements in the fields of AI, Machine Learning, cyber security, blockchain, behavioral analytics, Anti- Money Laundering (AML) on improving security in banks and detecting fraud [1][3][5][6][14].

There has been increase in the accuracy of AI-based models to detect abnormal transactions, progress in cyber security frameworks to improve Authentication, access control, and security of data and transparency, traceability and integrity in financial transactions using blockchain technology [1][3][5][6][14].

However, some research gaps exist. Most of the traditional AML methods focus on detecting suspicious financial transactions after the transaction has taken place which is not sufficient in preventing financial loss instantly [9][10][11]. Existing cyber security frameworks also tend to focus on authentication of login credentials, network security and user access control without analyzing the transactional behavior of customers [2][4][8][20].Although several recent research works propose AI based transaction monitoring and anomaly detection methods, these models focus solely on analyzing transactions only and very few works explore the integration of both cyber security monitoring and AML based transaction analysis for verification of both the customer and the legitimacy of the transaction before authorizing payment [5][6][7][12].

Another research gap observed is the limited use of combined analysis of behavioral parameters like user login IP address, device type, login location, login time and past user transaction history with transaction patterns. Existing works tend to fail to combine these login actions with transaction patterns to detect fraud before transaction takes place [6][15][16].

The proposed "Cyber-Integrated Anti-Money Laundering System for Pre-Transaction Fraud Prevention" addresses these research gaps by providing a single intelligent framework for cyber security monitoring, behavioral analysis, anomaly detection, and AML based transaction analysis. The proposed system monitors user login behavior constantly, uses Artificial Intelligence to analyze the transactional behavior, generate real-time alerts, and prompt the user for further verification before transaction. The aim is to reduce financial fraud, enhance banking security and compliance and building up the customers' trust in digital transactions [1][5][9][12][20].

IV. Discussion

This survey of relevant literature proved that AI, ML, cybersecurity, blockchain technology, and behavior analytics helped greatly improve fraudulent detection in present-day banking.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 10, October 2026)

Studies of AI-based fraud prevention systems have proven how the technology performs excellent in Detecting abnormal transactions, minimizing false alarms rates and augmenting decisions with predictions. Learning by adaptation for machine learning helps it catch and prevent evolving fraudulent behaviors unlike the traditional rule based techniques for fraudsters prevention. In line with this, cybersecurity plays a significant role in modern digital banking with the monitoring of your customer's personal and other security details, unauthorized login patterns, authentication protocols, and unauthorized actions while blockchain has been proved and recognized as more stable since a decentralized and immovable source of financial data stores it providing immutability. Even though all these three have their respective roles in achieving Financial Security, literature proves that Most of the available study focus on solving individual security problem rather than providing solution for prevention of fraud in a holistic manner. Mostly AI-based systems analyzes only behavior of transactions. On the flip side, the cybersecurity framework focuses only on analyzing login/authentication. Blockchain mechanisms ensure secure but un intelligent behavioural analytics to detect the fraudulent.Moreover the comparing shows us that few have attempted combining blockchain and ArtificialIntelligence as a security technology. These are mainly centered on providing governance policy and compliance, Financial risk management, policy, governance as a mechanism of AML, policy against cyber crime. Only two have tried to cover Anti-Money Laundering and Cyber, though they focused only on governing financial system compliance and policies, rather than real-time pre – transaction fraudPrevention. Hence, in an attempt to addressing these limitations in security in a much comprehensive manner ,The Cyber – Integrated AntiMoney Laundering System focuses on how the monitoring system of a customer's login, authentication details, transaction's behavioural patterns. The transaction patterns along with a behavioural analytics of every login attempts and prior validation of cyber identity of such transactions are being addressed in theCyber–Integrated AntiMoney Laundering System. It seeks to identify if a person logginto the bank account attempting to carry out transaction has legitimate identity or has been compromised with the malicious intention of performing Financial transactions after identification of suspicious behavior, requesting appropriate verification from customers before completing the payment process to detect any Cybercrime from their Financial Transactions prior to being a victim.

V. Conclusion

Due to recent development and increased in digital banking and online financial services, there is an increase in the risk of Cyber Fraud, unauthorized access into account, identity theft and money laundering schemes. Though Anti-Money Laundering system and traditional cybersecurity has strengthened the bank's security it mainly acts individually for different transaction processes by detecting the fraudulent activity post completion of the transaction which may increase loss for organization and customer. Literature Survey In this paper the literature survey on current work in the domain of Artificial Intelligence, Machine learning, Cybersecurity, blockchain and anomaly detection along with behavioral analytics and Anti-Money Laundering system used in current banking domain were discussed. From these literature's, we concluded that AI helps to improve the accuracy of identifying the fraud, Cybersecurity enhance authentication of customer and prevent them by intruders, blockchain secures all transactions data.

However most of the current research focused on different security system separately, and did not present an integrated system to analyze login behavior as well as transaction analysis before payment occurred. Conclusion and Future Scope Considering the issues and shortcomings of current techniques discussed in literature review, In this paper we proposed 'Cyber-Integrated Anti-Money Laundering system for Pre-Transaction Fraud prevention which integrate Cybersecurity' with 'AML transaction'. Using this system we will monitor login behavior of user and transaction behavior, along with intelligent based detection for anomalies and generating alerts. An alert will then request the user for additional user authentication in case of high suspicious level before executing the transaction. We can integrate some advance such as DL, graph based detection, federated learning, Zero trust security, Explainable AI (XAI) and blockchain based audit trail.

Acknowledgment

The authors would like to thank their project guide and faculty members for their valuable guidance and support. We also acknowledge the researchers whose work has contributed to this study.

REFERENCES

[1] FRAUD-X: An Integrated AI, Blockchain, and Cybersecurity Framework With Early Warning Systems for Mitigating Online Financial Fraud: A Case Study From North Macedonia.

[2] Cybersecurity Strategies For Safeguarding Customers' Data and Preventing Financial Fraud in the United States Financial Sectors.

[3] Advances in Cybersecurity Strategies for Financial Institutions: A Focus on Combating E-Channel Fraud in the Digital Era.

[4] The Inter-Role of Cybersecurity, AI and Blockchain in Preventing Money Laundering and Terrorism Financing.

[5] Detecting Insider Threats in Banking using AI-Driven Anomaly Detection with a Data Science Approach to Cybersecurity.

[6] Artificial Intelligence in Cybersecurity and Digital Finance.

[7] Defending Against Fraud: Cyber Fraud Detection and Prevention Techniques.

[8] A Comprehensive Framework for Strengthening USA Financial Cybersecurity: Integrating Machine Learning and AI in Fraud Detection Systems.

[9] Zero Trust Cybersecurity: Critical Success Factors and a Maturity Assessment Framework.

[10] Fraud Detection: A Systematic Literature Review of Graph-Based Anomaly Detection Approaches.

[11] AI-powered Financial Crime Prevention with Cybersecurity, IT, and Data Science in Modern Banking.

[12] AI-Driven Cybersecurity in Online Banking: Enhancing Fraud Detection and Risk Mitigation.

[13] AI-driven Fraud Detection in Banking: A Systematic Review of Data Science Approaches to Enhancing Cybersecurity.

[14] Cyber Security and Internet Banking: Issues and Preventive Measures.

[15] Cybersecurity Risks in Online Banking: A Detailed Review and Preventive Strategies Application.

[16] Mitigating Cyber Risk in Financial Institutions: Leveraging AI-Powered AML, Fintech Innovation and Seamless Financial Services for Security and Compliance.

[17] AML Compliance Under Pressure: Balancing National Security and Financial Inclusion.

[18] Enhancing Anti-Money Laundering and Counter-Terrorist Financing Strategies through Integrated Cybersecurity and Compliance Measures.

[19] An Integrated Cybersecurity and Anti-Money Laundering Governance Framework for Financial Crime Prevention.

[20] The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance.