Journal of Intelligent Systems and Internet of Things
Vol. 13, No. 02, PP. 256-271, 2024
DOI: https://doi.org/10.54216/JISIoT.130221

Innovative Approaches to Bank Security in India: Leveraging IoT, Block chain, and Decentralized Systems against Loan Scams

Akhtar Hasan Jamal Khan[1], Syed Afzal Ahmad[1,*]
[1]Department of Computer and Business Management, Integral University, Lucknow, India
Emails: ahjk@student.iul.ac.in; safzal@iul.ac.in

Abstract

This research paper explores the significant impacts of multiple loan fraud on Indian banks and financial institutions, emphasizing the resulting bad debts and financial losses. The issue is exacerbated in the real estate sector, where influential developers exploit system vulnerabilities to secure multiple loans using the same collateral. Consumers also face challenges in accessing credit due to these fraudulent practices. The study underscores the need for enhanced regulatory measures and internal controls within financial institutions. Additionally, it introduces IoTBlockFin, a decentralized system that integrates block chain and IoT technologies to securely assess customer reliability and mitigate fraud. IoTBlockFin's Advanced Proof of Work (APOW) mechanism, combined with IoT data for real-time monitoring, offers superior security, latency, and cost-effectiveness compared to centralized systems, as demonstrated by experimental results.

Received: January 25, 2024 Revised: February 21, 2024 Accepted: April 01, 2024

Keywords: IoTBlockFin; Scams; Decentralize System; Flask architecture; SMOT; APOW

1. Introduction

In simple terms, a home loan from a bank involves using property or real estate as collateral. It's an agreement where the borrower receives money from the lender to purchase a home and then repays the loan (with interest) over a specified period. Real estate includes land, buildings, and natural resources like minerals, agriculture, or water, encompassing both immovable property and interests in such property. Real estate may be divided into four categories: land, commercial, industrial, and residential. The real estate sector involves producing, buying, and selling property, playing a crucial role in economic growth. Home loans are vital in this business, enabling buyers to purchase properties through manageable instalments and attracting customers who lack sufficient cash. Because of this backing, the real estate market grows quickly and there is a continual flow of cash. The finance industry is very vulnerable to fraud, particularly in the loaning sector. In a developing economy, multiple borrowing is typical, when consumers look for loans from several lenders when one lender is unable to satisfy their credit needs [1, 2, 3]. When a borrower obtains numerous loans from different institutions using the same collateral, they may commit multiple loan fraud, which involves misleading the lenders [4-5]. Banks and other financial institutions suffer large annual losses as a result of these crimes [6]. According to the data for March 2021, 90 banks and financial organizations stated 45,613 cases of fraud in loan issuance with a total amount of approximately 5 trillion INR, or 4. Five per cent of the total bank credit portfolio as per the Reserve Bank of India (RBI) study. The largest fraud amount was disclosed by the largest lender in the nation, the State Bank of India (SBI), which was more than INR 78,000 crore [7]. Such startling figures inflict a greatly negative impact on India's economy as a developing country. There is a need to come up with a good system that will prevent such kinds of fraud from happening. This

paper shall seek to identify how multiple loan fraud is prevalent in India and what measures may be taken to contain it. Within the framework of the financial situation in India, loan fraud has recently emerged as the most critical issue affecting the banking sector and, consequently, the financial institutions' profitability. These scams pose a grave threat to the stability and sustainability of the banking industry in India as they are characterized by unscrupulous credit practices and credit risk fraud. This paper focuses on the various aspects of loan fraud in India and seeks to shed light on the myriad impacts they have on the bank's financial performance. This study's content is organized into multiple sections: the first section of the paper presents the context of the investigation; the second section uses secondary data like surveys, case studies and research papers to establish the key factors that define the study; the third part explains how statistical analysis has been used on the primary data from the survey conducted in various banks in Uttar Pradesh, India; the fourth part describes the IoTBlockFin architecture that incorporates blockchain and IoT to design coping mechanisms; the last part recapitulates the.

2. Related Work

I've compiled a Literature Review from various sources including research articles, case studies, books, newspapers, published theses, websites, and online surveys. The selection process involved using keywords such as "Bank Scams," "Financial Frauds," "Loan Scams," "Bank Frauds," and "Multiple Loan Scams" across databases like K-Hub, ProQuest, Ebsco, IEEE, Springer, Elsevier, IIM Bangalore, Google Scholar, Journal of Public Affairs, and Shodhganga press. Additionally, I gathered data on scams from a report by the Reserve Bank of India (RBI) and various newspapers such as TOI, The Tribune, Indian Express, Mid-Day, The New Indian Express, Hindustan Times, and Hindu News. International online survey websites like Deloitte.com and Statista.com were also consulted. To ensure the research's relevance, papers primarily from the years 2007–2023 were selected. Approximately 150 papers related to bank scams were reviewed, with citations drawn from approximately 70 publications, 11 theses, 10 case studies, and online surveys focused on loan scams.

Table 1: Type of Research

Author	Year	Contribution	country	Methodology
S. Prasanth [8]	2021	Examining the Impact of Growing Non-Performing Asset Levels on the Bank's Worsening Financial Situation Following COVID	India	Exploratory study
Saha, M.[9]	2021	Report on loan fraud	India	Survey
Onukwugha, C., &Amanze[10]	2018	System for Detecting Loan Fraud in the Banking Sector	Nigeria	Data Mining
Mia, A.[11]	2017	Causes of Multiple Borrowing in Microfinance	Bangladesh	Survey
Mungure[12]	2015	Causes and Impacts of Loan Default on Microfinance Institutions Activities	Tanzania	Case Study
Ajah, I. A., &Inyiama, H.C.[13]	2011	Examined the benefits of several information technology applications in reducing the issues associated with loan fraud.	Nigeria	Application of IT
Krishnaswamy, K.[14]	2007	Multiple borrowing and competition in the Indian microfinance industry	India	Survey
Chaudhary, N., & Gupta, R.[15]	2020	Impact of COVID-19 on loan default rates: A comparative analysis	India	Quantitative analysis
Ojo, O. O.[16]	2019	Digital banking fraud prevention techniques: a case study of Nigerian banks	Nigeria	Case Study
Rahman, M.[17]	2016	Role of credit scoring models in predicting loan default: Evidence from Bangladesh	Bangladesh	Quantitative analysis
Gomez, P. S., et al.[18]	2014	Development and implementation of a fraud detection system in Latin American banks	Multiple	Case Study
Wang, L., et al.[19]	2023	Machine learning approaches for real-time fraud detection in the Chinese banking sector.	China	Machine Learning

2.1 Main Cause of Loan Scam

After reviewing several papers I found that these can be the main cause of Bank scams that are listed here: Employees lack the necessary training to detect bank scams, according to Ashu Khanna (2009) [20]. Employee compliance and attitude toward RBI procedures are both positively impacted by training. Bhasin, M. L.(2015)[21] Ineffective staff training programs and bad employment practices exist; often poor internal control mechanisms, overworked employees, and low compliance among bank managers, offices, and clerks. "According to Bhasin et al. (2016)[23] and Gupta and Gupta (2015)[22], although elements include subpar work practices, The most important factors increasing the likelihood of fraud were shown to be inadequate internal control mechanisms and inefficient staff training, According to research by Khanna and Arora (2009), Ganesh and Raghurama (2008), and Livshits et al. (2015), staff members who are overworked and lack training, Low levels of compliance and competitiveness were the primary causes of bank frauds. In 2019[24], Shah, M., and Mittal, A. Employees at banks have relatively little knowledge about bank fraud. M. L. Bhasin. (2015)[23] Staff members frequently lack a precise understanding of what constitutes fraud, thus they must be trained on this topic. Consequently, staff members should regularly get training sessions and an overview of global best practices for early fraud identification and prevention. Regular e-module releases with e-certifications and upgrades are possible. Neha Sharma (2018) [25] states that employee (including management) negligence in adhering to standard procedures was the most common cause of the rise in fraud. Employees are under pressure to reach their goals. Inadequate resources for identifying warning signs. Illegal collaboration between workers and other parties. Additional causes include a decentralized banking system, improper or infrequent audits, and a failure to properly verify security documentation. Non-verification of the money's final usage, Multiple financing to the same party against the same security, inadequate supervision inadequate pay for staff members, inadequate internal control framework extension of credit facilities without authorization, and Coordination between workers and outside parties.

2.2 Case Study

In Below Table 2, we have briefly discussed a few cases that were reported in various newspapers:

Table 2: Case Studies

Case Reference	**Year**	**Bank**	**Amount**	**Scammer**	**Scam Type**
Hindustan Times Delhi	24 March 2021	DHFL	2 lakh fake home loan accounts	Bank Employee and owner	Type1(only bank)
Neha Sharma, Technology Management Journal for Increasing Economic Growth, Volume 9, pages 71–88	April 2018	Allahabad Bank	52 lakhs	Customer, Forged documents	Type 3
Neha Sharma, Technology Management Journal for Increasing Economic Growth, Volume 9, pages 71–88	April 2018	State Bank of Patiyala	5 crore	Customer, Bank employee, Forged documents	Type1 &Type 3
Neha Sharma, Technology Management Journal for Increasing Economic Growth, Volume 9, pages 71–88	April 2018	Syndicate Bank	209 Crore	Customer, Bank employee, forged documents, Third party	Type1& Type2 & Type3 & Type 4
Neha Sharma, Technology Management Journal for Increasing Economic Growth, Volume 9, pages 71–88	April 2018	Punjab & Sind Bank	86 Lakhs	Customer, forged documents	Type3
NiravModi Case studyPramana Research JournalVolume-9, Issue-6	2019	Punjab National Bank	12,700 Crore	Customer, Bank Employee	Type1
Times of India Ghaziabad	16 March 2021	Punjab National bank	47.22 Lakhs	Customer, Bank Employee, Forged document	Type 1, 3 & 4

www.moneycontrol.com/news	22 July 2021	Karuvannur Co-op Bank scam-Kerala	100 Crore	Bank Employee, Outsider	Type 5
The new Indian Express -Telangana	8 Jan 2022	Union Bank of India	2 Crore	Bank Employees, Outsider(Broker	Type 5
Times of India Ghaziabad	23 Dec 2021	Punjab National Bank	450 crore	Customer, Bank Employee, outsider	Type 1 & 5
The Hindu news Chennai	30 Sep 2021	HSBC BANK	1.51 Crore	Customer, Bank Employee, Forged Documents	Type 1, 3 & 4

2.2.1 Findings of Case Study: Classification of Loan Fraud

After going through several papers and case studies I observed that there can be five types of Loan fraudulent that are classified based on the people's connivance of scam.

Type 1. Scams committed by customers in connivance with bank employees.

Type 2. Scams committed by customers in connivance with third party.

Type 3. Scams committed by customers with the help of fake/Manipulated/Duplicate documents.

Type 4. Scams committed by customers in connivance with vendors.

Type 5. Scams committed by Outsider in connivance with bank employee

2.3 Survey

The survey Report is shown in graph 1, In "Statista, 2024," which displays the total number of bank fraud cases in India from the 2009–2024 fiscal year.

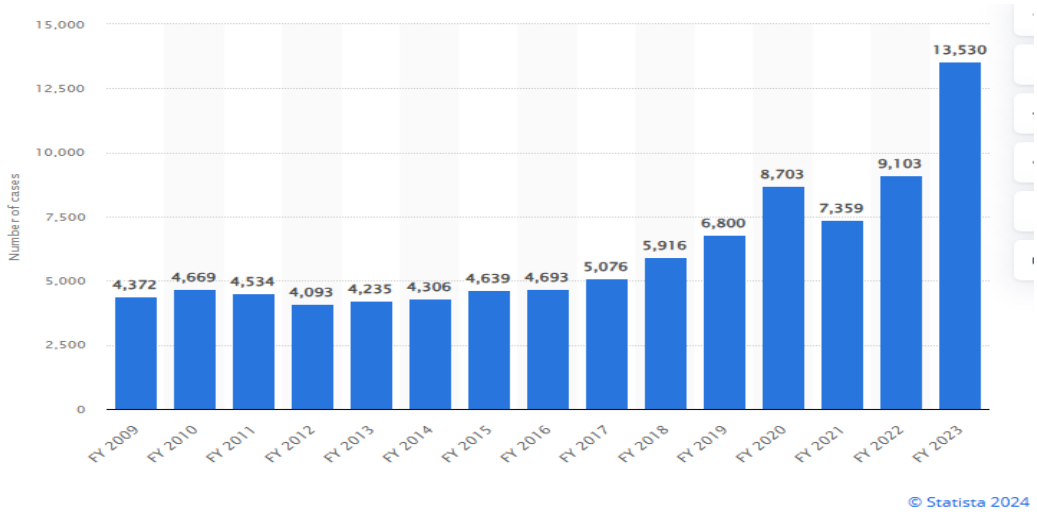

Figure 1. Total number of bank fraud cases in India from 2009 to 2024 (Source): India-number-of-bank-fraud-cases, January 2024 (https://www.statista.com/)

Per an article presented in the "India Banking Fraud Survey" by Deloitte India, 78% of respondents to "Edition IV" (2024) predict an increase in banking sector scams during the next two years, Loan fraud will account for 24%, of mobile and online banking fraud for 14%, and identity and data theft fraud for 12%.

2.3.1 Findings of Survey Review

Recognizing the present state of fraud in the banking industry (2019–2024) Given what is stated in "Section I: The presentation "Understanding the Current Fraud Environment in the Banking Sector" was made at Deloitte at the "India Banking Fraud Survey, Edition IV. The COVID-19 pandemic coincided with a period of rising bank fraud incidences that the banks were finding difficult to handle. A global increase in financial crime is anticipated because of the unpredictability of the corporate environment. The economic downturn has only increased the danger of fraud and money laundering for institutions.

2.4 Impact of Major Factors Leading to Loan Scams in the Indian Banking Industry, especially in Uttar Pradesh

After conducting an extensive literature review, it is clear that numerous factors contribute to loan scams in the Indian banking industry, particularly in Uttar Pradesh. However, the most significant factors identified are:

2.4.1 Role of Employee Compensation in Bank Loan Scams

Out of the several causes of loan scams within the banking industry, employee remuneration stands out as being a major reason. As it is stated in the available literature, workers, who get less pay and few incentives and bonuses for their performance, have low morale and make ethical failures. Under compensation may cause bank workers in Uttar Pradesh where they may experience other socioeconomic issues to engage in fraud or otherwise overlook it. Organizational internal fraud can be reduced if organizations address the pay concern which is the disparity of salary and other incentives to industry standards and ethical benchmarks.

2.4.2 Role of Third-Party Interference in Bank Loan Scams

Outside interference is one of the most common aspects of loan scams. In regard to loans, external participants such as brokers, middlemen and other similar entities often exploit the situation by collaborating with the banks' employees or presenting fake proofs. Uttar Pradesh is particularly susceptible to such interference mainly due to possible weak compliance and oversight. To mitigate this risk, it is essential to strengthen the protection of regulations, improve the quality of due diligence, and pay more attention to the activity of third parties.

2.4.3 Assessment of Document Validation and Authentication in Loan Proposals

The validation and authentication of documents are very important to put an end to loan scams. The available literature shows that lack of proper procedure for identification, inconsistency in the measures and lack of proper training for the personnel are some of the major drawbacks. The above problems are compounded by poor verification technology that is still old-fashioned in Uttar Pradesh. Loopholes in the procedural systems that enable fake loan application forms to be processed. Measures that would help increase the loan approval credibility are the following: the processes should be made as uniform as possible, the training of the employees should be enhanced, and the verification technologies should be updated. The analysis of the literature is done such that it shows that staff remuneration, third-party intervention, and document validation and authentication are some of the factors that are influencing loan scams in the Indian banking industry, especially in Uttar Pradesh. Through purposeful reforms, well-measured actions and enhanced regulatory surveillance, the banking industry might substantially decrease the rate of loan fraud by addressing these problems. This will enhance the financial stability and systemic trust among the people of the country.

3. Proposed Method

This research adopts a systematic approach to investigate the phenomenon of loan scams in the banking sector. This is done through the collection of survey data, analysis, and technology advancement. First, primary data collection is made on loan scams and their facets prevalent in Uttar Pradesh's public and private sector banks. However, before the actual data is collected, normality tests are conducted on the data set to ensure that it meets all the requirements of a parametric test. This is followed by a statistical analysis using an Analysis of Variance (ANOVA) test that shows significant variations in the factors leading to loan scams within the banks. The conceptual framework regarding the use of blockchain technology for loan processing is developed to provide suggestions to take preventive measures for making automation, security and transparency better. This methodology provides realistic measures against loan scams in the banking sector by integrating modern technical solutions with statistical analysis. These findings suggest the proposed method's potential for significant advantages in real-world IoT applications.

Algorithm 1: Decentralized Data Storage

Step 1: Data Collection from IoT Devices
Collect raw data from IoT devices:
$D = \{d_1, d_2, \dots, d_n\}$ (1)
Identify data type and source for each data point:
$d_i = (type, source)$ (2)
Aggregate data into a structured format:
$D_{agg} = \sum_{i=1}^{n} d_i$ (3)
Step 2: Data Encryption
Generate a symmetric key K :
$K = \text{KeyGen}()$ (4)
Encrypt the aggregated data using the symmetric key:
$E_D = \text{Enc}(K, D_{agg})$ (5)
Step 3: Data Segmentation
-Split the encrypted data into smaller segments:
$\{S_1, S_2, \dots, S_m\} = \text{Segment}(E_D)$ (6)
-Determine segment size:
$|S_i| = \frac{|E_D|}{m}$ (7)
-Ensure all segments are of equal size:
$S_i \approx S_j \quad \forall\, i, j \in \{1, \dots, m\}$ (8)
Step 4: Hashing Segments
Generate a hash for each data segment:
$H_i = \text{Hash}(S_i)$ (9)
Step 5: Data Redundancy
-Create redundant copies of each segment for fault tolerance:
$S_{ij} = \text{Copy}(S_i) \quad \forall\, j \in \{1,2, \dots, r\}$ (10)
-Ensure multiple copies:
$r > 1$ (11)
-Maintain consistency:
$H_{ij} = H_i$ (12)
Step 6: Distributed Storage
-Distribute the segments across different blockchain nodes:
$\text{Node}_k \leftarrow S_{ij}$ (13)
$\text{Nodes} = \{\text{Node}_1, \text{Node}_2, \dots, \text{Node}_p\}$ (14)
$p \geq r$ (15)
Step 7: Index Creation
-Create an index for easy retrieval of segments:
$\text{Index}(D_{agg}) = \{H_1, H_2, \dots, H_m\}$ (16)
Step 8: Index Storage on Blockchain
-Store the index on the blockchain for transparency:
$\text{Blockchain} \leftarrow \text{Index}(D_{agg})$ (17)
-Ensure immutability:
$\text{Index}_{\text{hash}} = \text{Hash}\left(\text{Index}(D_{agg})\right)$ (18)
-Use a smart contract for index management:
$SC_{\text{index}} = \text{Deploy}\left(\text{Index}(D_{agg})\right)$ (19)
Step 9: Data Request Initiation
-Initiate a data retrieval request by querying the blockchain:
$\text{Request}(D_{agg})$ (20)
Step 10: Segment Retrieval from Nodes
Retrieve the segments from the respective nodes:
$S_{ij} \leftarrow \text{Node}_k$ (21)
Step 11: Validate Segment Integrity
-Validate the integrity of each retrieved segment:
$\text{Valid}(S_{ij}) = \text{CheckHash}(H_{ij}, S_{ij})$ (22)
Step 12: Segment Decryption
-Decrypt the segments using the symmetric key:

$S_i = \text{Dec}(K, S_{ij})$ (23)

-Ensure all segments are decrypted correctly:

$S_i = S_j \quad \forall\, i, j$ (24)

-Reconstruct encrypted data:

$E_D = \sum_{i=1}^{m} S_i$ (25)

Step 13: Data Reassembly

Reassemble the segments to form the encrypted data:

$E_D = \{S_1, S_2, \ldots, S_m\}$ (26)

Step 14: Final Decryption

Decrypt the reassembled data using the symmetric key:

$D_{agg} = \text{Dec}(K, E_D)$ (27)

Step 15: Verify Data Integrity

Verify the integrity of the decrypted data:

$\text{Verify}(D_{agg}) = \sum_{i=1}^{n} \text{Check}(d_i)$ (28)

-Cross-check with original data:

$\text{Match}(D_{agg}, D)$ (29)

-Ensure no data loss:

$\sum_{i=1}^{n} d_i = \sum_{i=1}^{n} d_i'$ (30)

Step 16: User Notification

Notify the user of successful data retrieval and integrity check:

$\text{Notify}(\text{User,Status})$ (31)

Step 17: Data Utilization

Use the verified data for intended applications:

$\text{Utilize}(D_{agg})$ (32)

Distributed storage protects Internet-of-Things data. This approach efficiently distributes data storage between nodes utilizing blockchain technology. We use symmetric keys to encrypt and protect Internet of Things data. After encryption, decoding reduces data. We then hash the components to guarantee their unique identification. To ensure fault tolerance and redundancy in the blockchain, we use a distributed architecture with many nodes. Using a blockchain index, we can find segment hashes. In response to data retrieval requests, we extract relevant segments from nodes and compare their hashes to the index. We must inspect, decrypt, and reassemble individual portions before recovering encrypted data. To decrypt data delivered via the Internet of Things, use a symmetric key. This technology protects data availability and integrity by eliminating a single point of failure and allowing for distributed storage and retrieval. Removing vulnerabilities may have additional benefits.

Algorithm 2: Secure Communication Protocols

Step 1: Input from Algorithm 1

-Receive encrypted data segments S_i and their hashes H_i:

$S_i = \{S_1, S_2, \ldots, S_m\}$ (33)

$H_i = \text{Hash}(S_i)$ (34)

-Retrieve symmetric key K for decryption:

$K = \text{RetrieveKey}()$ (35)

$E_D = \text{Dec}(K, S_i)$ (36)

Step 2: Key Generation

-Generate public-private key pairs for devices:

$(PK_i, SK_i) = \text{KeyGen}(i)$ (37)

-Exchange session keys using public keys:

$SK_{ij} = \text{Enc}(PK_j, K_{ij})$ (38)

$K_{ij} = \text{SessionKey}(PK_i, PK_j)$ (39)

-Encrypt the aggregated data using the session key:

$E_D' = \text{Enc}(K_{ij}, E_D)$ (40)

$E_M = \text{Enc}(K_{ij}, M)$ (41)

$Sig_i = \text{Sign}(SK_i, H(M))$ (42)

Step 3: Data Transmission Initiation

-Transmit the encrypted data and signature:

$\text{Transmit}(E_M, Sig_i)$ (43)

$M \rightarrow \text{Node}$ (44)

Step 4: Data Receipt by Blockchain Node

-Receive the encrypted data and signature:

$\text{Receive}(E_M, Sig_i)$ (45)

Step 5: Signature Verification
-Verify the received signature using the sender's public key:
$V = \text{Verify}(PK_i, Sig_i, H(M))$ (46)
$V_i = \text{VerificationStatus}(PK_i)$ (47)
$\text{Check}(V)$ (48)
Step 6: Data Decryption
-Decrypt the received message using the session key:
$M = \text{Dec}(K_{ij}, E_M)$ (49)
Step 7: Data Validation
-Validate the integrity of the decrypted message:
$H_{recv} = \text{Hash}(M)$ (50)
$\text{Valid}(M) = (H_{recv} == H(M))$ (51)
Step 8: Session Key Management
-Generate new session keys periodically:
$K'_{ij} = \text{NewSessionKey}$ (52)
$(PK_i, PK_j)K_{ij} \leftarrow K'_{ij}$ (53)
Step 9: Secure Channel Establishment
-Establish a secure communication channel:
$\text{Channel}_{sec} = \text{Establish}(PK_i, PK_j)$ (54)
Step 10: Continuous Monitoring
-Monitor the communication for anomalies:
$\text{Monitor}(M)$ (55)
$\text{Anomaly} = \text{DetectAnomaly}(M)$ (56)
Step 11: Anomaly Detection
-Trigger alerts upon detecting anomalies:
$\text{Alert} = \text{AnomalyDetected}(\text{Anomaly})$ (57)
$\text{Notify}(\text{Admin})$ (58)
$\text{Log}(\text{Anomaly})$ (59)
Step 12: Data Integrity Checks
-Perform periodic data integrity checks:
$H_{chk} = \text{Hash}(M)$ (60)
$\text{CheckIntegrity}(M) = (H_{chk} == H(M))$ (61)
Step 13: Data Encryption for Transmission
16. Encrypt data for transmission:
$E_M = \text{Enc}(K_{ij}, M)$ (62)
Step 14: Signature Generation for Transmission
-Generate digital signature for encrypted data:
$Sig_i = \text{Sign}(SK_i, H(E_M))$ (63)
$\text{Transmit}(E_M, Sig_i)$ (64)
$\text{LogTransmission}(E_M, Sig_i)$ (65)

IoT sensors and devices, as well as blockchain nodes, use secure communication protocols to authenticate and encrypt data. Algorithm 1 initializes hashes and encrypted data segments. We create device public-private key pairs once we obtain a symmetric data decryption key. To share session keys and encrypt the resulting data, we use public keys. We use the sender's private key to create a digital signature, which we then send to the blockchain node. Additionally, encrypted data is provided. Using the sender's public key, the node instantaneously confirms the signature's validity. The chat is then decrypted using the session key. We will compare various message hashes to confirm transmission. We create a huge number of new session keys every day to boost system security. An added benefit is a secure communication route between devices. Continuous attention enables rapid detection of irregularities. Specific data integrity tests verify the data's validity. To complete the Internet of Things ecosystem communication protocol security and authorization process, we re-encrypt and sign the provided data.

Hypothesis and Descriptive Data for the Variable "NPA"

Hypothesis 1: There is no significant relationship between employee compensation and bank loan scams.

It is necessary to note that all the hypotheses were tested with the help of the variable “NPA” and its descriptive data are given in Table 3 according to the categories of the variables. The categories are identified with the help of numbers that are on a scale of 1. 43 to 5. 00, along with basic statistics, including N, mean, SD, SE, and 95%

CI of the mean and min and max values. For instance, the mean values range from 1.0000 to 1.5972, indicating variations in average values among different categories. The standard deviation values range from 0.0000 to 1.15470, reflecting the dispersion of data points around the mean within each category. This table provides insights into the distribution and variability of the "NPA" variable, aiding further analysis and interpretation.

Significance of Employee Compensation and Bank Loan Scams

Table 3 shows the ANOVA results, indicating a significant relationship between employee compensation and bank loan scams. The F-statistic of 2.235 and p-value of 0.005 suggest significant differences in the incidence of loan scams across different levels of employee compensation. The null hypothesis is rejected, confirming that employee remuneration plays a discernable role in determining the prevalence of loan scams.

Table 3: Significance

ANOVA					
NPA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	12.843	15	.856	2.235	.005
Within Groups	204.942	535	.383	Within Groups	204.942
Total	217.785	550		Total	217.785

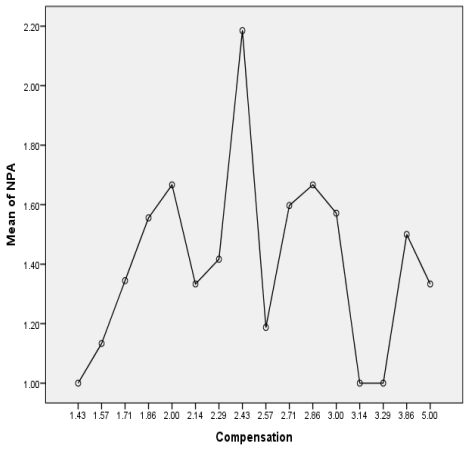

Figure 2. Employee Compensation and Bank Loan Scams

Hypothesis 2: There is no conclusive link between bank loan schemes and third-party intervention.

Table 3 provides descriptive data for the variable "NPA" across different categories, with specific values ranging from 1.00 to 3.43. The table includes the number of observations (N), mean, 95% confidence interval for the mean, standard deviation, standard error, and lowest and highest values for each category. For instance, there are 467 observations in the 3.14 category, with a mean of 1.3776 and a standard deviation of 1.17372. This table helps in understanding the distribution and features of the "NPA" variable within each category and the overall dataset.

Significance of Third-Party Interference and Bank Loan Scams

Table 6 displays the ANOVA results, showing a significant relationship between third-party interference and bank loan scams. With an F-statistic of 2.859 and a p-value of 0.002, the findings indicate significant differences in loan scams attributed to variations in third-party interference. The null hypothesis is rejected, confirming the impact of third-party interference on the incidence of loan scams.

Hypothesis 3: Document validation and authentication do not significantly impact the approval of bank loan proposals.

Table 4 presents descriptive data for the variable "NPA" across various categories, with values ranging from 1.00 to 3.00. The table includes the number of observations (N), mean, lowest and maximum values, 95% confidence range for the mean, standard deviation, standard error, and. For example, in the category labeled 2.71, A mean of 1.4000 and a standard deviation of 0.89316 are found in 60 observations. There are 551 observations in the entire dataset, with a mean of 1.4144 and a standard deviation of 1.11350.

Significance of Document Validation and Authentication

Table 8 shows the ANOVA results, revealing a statistically significant impact of document validation and authentication on the approval of bank loan proposals. With an F-statistic of 2.186 and a p-value of 0.022, the

results indicate that variations in document validation and authentication significantly influence loan proposal approvals. The null hypothesis is rejected, underscoring the importance of these procedures in the lending decision process**.**

Table 4: Significance

ANOVA					
NPA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	23.931	9	2.659	2.186	.022
Within Groups	658.003	541	1.216		
Total	681.935	550			

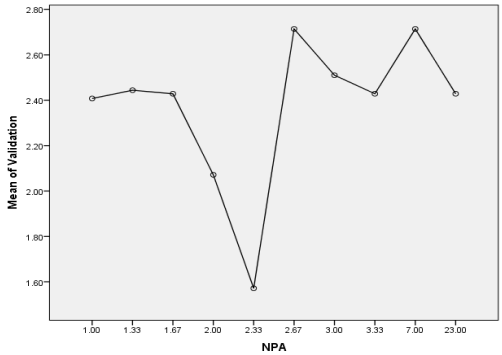

Figure 3. Third Party and Bank Loan Scam

4. Preventive and Coping Strategies for Loan Scams

Numerous banks and financial institutions continuously face the persistent problem of multiple loan scams, which affect various sectors beyond real estate. These scams lead to substantial annual bad debts and significant financial losses for lenders. Although AI-powered solutions for predicting loan scams have recently emerged, challenges persist, especially when privacy breaches occur, potentially altering AI model decisions. In this study, we address these challenges by implementing a blockchain network on a localized server to conduct loan fraud detection directly on the generated nodes. This approach ensures the confidentiality of the deployed model, as both training and prediction occur within the blockchain network. We use Proof of Work (POW) as the consensus mechanism for this blockchain network, which is established on a Flask server, providing a robust infrastructure for our research. For our experiments, we use a banking loan dataset with 36 features, using Support Vector Machine (SVM) and Naive Bayes Classifier, two traditional machine learning techniques, for testing and training. Our findings show that SVM outperforms the Naive Bayes Classifier, achieving 99% accuracy in both the training and testing phases. This promising approach not only enhances the detection of loan scams but also helps banks and financial institutions combat fraudulent loan management practices securely [26-17].

4.1 IoTBlockFin's Architecture

Blockchain is a system that enables multiple communication partners to conduct transactions without the need for a third party. These transactions are verified and validated by specialized nodes. Figure 4 illustrates the Blockchain architecture, where blocks or nodes are connected in a chain-like manner. Each block contains information such as the Header, Previous block address, Timestamp, Nonce, and Merkle Root [22]. The header is needed to find a specific block inside the large Blockchain, examining each block sequentially. During routine mining operations, miners change the nonce value to hash a block header. The block header includes details about three types of blocks. The ith block is linked to the preceding block using its hash, which serves as a pointer to the previous block's address. A timestamp provides proof of the authenticity of the data within a document, serving as a unique identifier for the time of creation. The nonce is a unique number critical for the block's proof of work. Miners compare the nonce to the current target to validate its value. The Merkle Root is a data structure composed of multiple data blocks, allowing for the unique identification of every transaction in a block, making Merkle Trees ideal for storing Blockchain data. Users can verify if a transaction is part of a block using this structure [23]. In the following section, the essentials of Blockchain Architecture are depicted: In Blockchain technology, a block acts as a core part of the network; this is a form of ledger that is used to store and protect transactions using the hash tree code. This structure is very important in supervising the numerous transactions that occur every day within the global arena. This idea ties these blocks by cryptographic hashes and shapes the basis of Blockchain

architecture. This interconnectedness is done through the 'hash' of the previous block, which makes it very hard to manipulate the records of the transaction. Consensus mechanisms are extremely important in decentralized systems such as cryptocurrencies since they are responsible for reaching a consensus of all agents or nodes in the current state of the network. They are crucial for record keeping and improving the fault tolerance of the systems. Our implementation uses Proof of Work (POW) as the selected consensus algorithm; it is a mechanism that validates new transactions and adds them to the Blockchain through a specified amount of computation [28].

4.2 Flask Architecture

Flask is one of the micro web frameworks for Python. Being a micro-framework, it does not work based on extra requisites such as compilers or libraries. Compared to the large frameworks, it does not provide elements that are normally offered by other libraries, for example, form validation mechanisms or database abstraction layers.

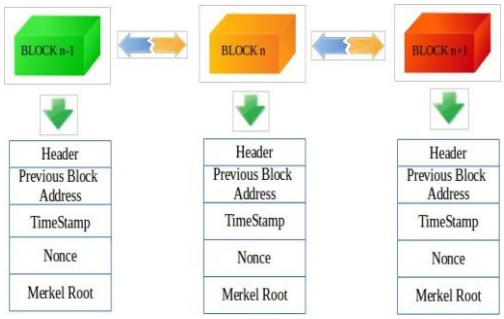

Figure 4. Flask Architecture

The Flask architecture, shown in Figure 4, is commonly used to implement adaptable security rules in operating systems. It primarily consists of an Object Manager (OM) and a Security Server (SS). To ensure a clear separation between decision-making and enforcement, OM and SS should be kept apart in practice. Figure 4 Flask Architecture The overall architecture and sequence of actions are illustrated in Figure 5. The process begins with dataset preparation and feature selection, with detailed preprocessing steps discussed in Section 4.3. After preparation, the dataset is split into training and testing sets. Notably, the dataset was found to be imbalanced and was subsequently balanced, as described in Section 4.4. Model training and testing were conducted on the Blockchain network. Once trained, the models' performance metrics, including accuracy and ROC curve, were computed and the results were returned to the client.

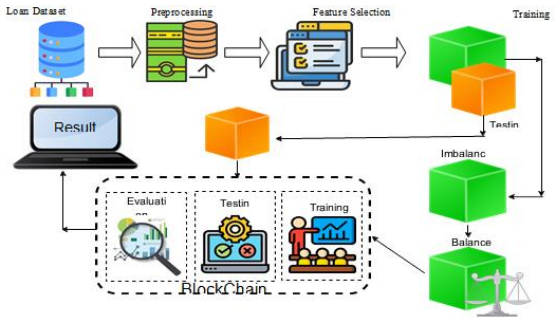

Figure 5. IoTBlockFin's Overall Architecture representing a sequence of actions

4.3 Dataset & Performance Evaluation

4.3.1 Dataset and Pre-processing

The dataset used for our experiments is a large-scale loan scam fraud detection dataset from Kaggle, featuring 36 attributes and one class attribute indicating loan status (0 for non-fraud, 1 for fraud). The dataset initially had 74,411 non-fraud records and 21,367 fraud records, indicating a significant class imbalance. To address this, we applied the Synthetic Minority Oversampling Technique (SMOTE), balancing the classes to 74,411 records each, resulting in 148,822 records in total. Additionally, we duplicated these records to further assist model adjustment, resulting in a final dataset of 297,644 records, with 148,822 for each class.

4.4 Results

We evaluated the performance of Naive Bayes and SVM models on this dataset. Performance before class balancing is shown in Table 5, while results after balancing are in Table 6. SVM achieved an overall F1-Score of 99%, outperforming Naive Bayes in terms of Precision, Recall, and F1-Score for both classes. On the imbalanced dataset, SVM achieved an F1-Score of 99% for class 0 and 50.4% for class 1. The confusion matrix for SVM (Figure 6) shows Minimal false positives and negatives. The AUC/ROC curve for SVM (Fig. 7) indicates a perfect classification performance with an AUC score of 1.0.

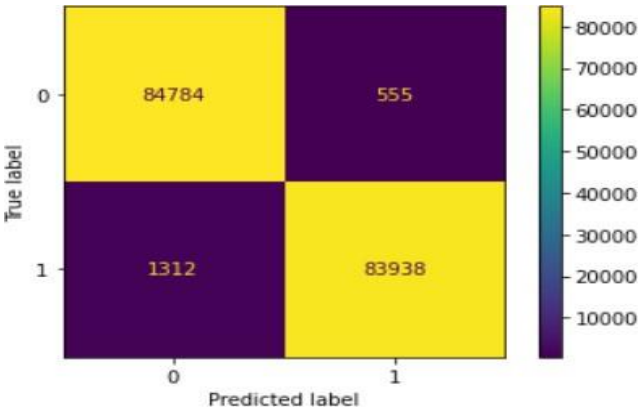

Figure 6. Confusion matrix

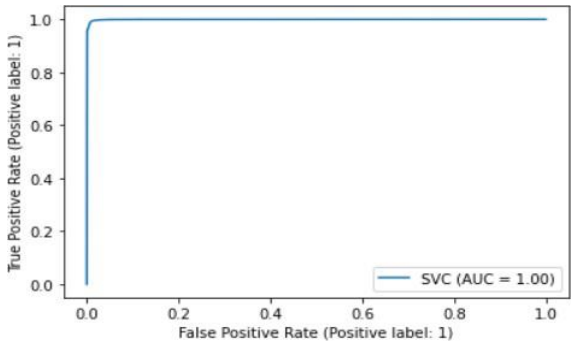

Figure 7. ROC/AUC Curve

Table 5: Performance Evaluation (Class Imbalance)

Model	**Naive Bayes**		**SVM**	
Metrics	**Class 0**	**Class 1**	**Class 0**	**Class 1**
Precision	0.94	0.57	0.94	0.60
Recall	0.91	0.55	0.98	0.56
F1-Score	0.92	0.56	0.96	0.58

Table 6: Performance Evaluation (Class Balance)

Model	**Naive Bayes**		**SVM**	
Metrics	**Class 0**	**Class 1**	**Class 0**	**Class 1**
Precision	0.95	0.94	0.98	0.99
Recall	0.92	0.95	0.99	0.98
F1-Score	0.94	0.95	0.99	0.99

The performance metrics of Naive Bayes and SVM models in forecasting loan frauds in various scenarios within the Indian banking sector are compared in Tables 1 and 2. Table 1 focuses on a class imbalance scenario, where instances of loan scams (Class 1) are significantly fewer compared to non-scam instances (Class 0). Naive Bayes and SVM show their efficiency in handling loan scams, and although they are quite similar, SVM has a slightly better precision and recall rate for Class 1. Particularly, SVM has a precision of 0. 60, and the recall is 0. 56 for Class 1, which shows that, in terms of the accuracy of separating real loan scams from the noise, it performs better than Naive Bayes. The F1-Score that preserves equal weights for Precision and Recall also depicts the efficiency of SVM with the values of 0. 96 for Class 0 and 0 for Class 1. 58 for Class 1, thus proving its efficiency in class imbalance situations. On the other hand, Table 2 shows the model performance when the class distribution is balanced with equal instances of scam (Class 1) and non-scam (Class 0). Here, both Naive Bayes and SVM perform well in terms of the precision, recall, and F1-Scores for both the classes, however, SVM is seen to be slightly better with values almost close to 1. SVM achieves precision scores of 0.98 for Class 0 and 0.99. In summary, while both models perform well in balanced scenarios, SVM consistently shows superior performance across all metrics in both balanced and imbalanced class settings, underscoring its robustness in accurately predicting loan scams in the Indian banking industry.

5. IoTBlockFin: Integration of IoT with BlochFin

According to studies (Surekha, N, 2022) [29–30], the banking industry contributes 70% of India's GDP, and to achieve its economic goals, India must accelerate this sector's growth to 8–10 times its current rate over the next decade. It takes two engines to achieve this ambitious growth: cutting-edge technology a scalable, tech-enabled system, and a secure banking system. An effective way forward is to combine Blockchain Technology (BCT) with Internet of Things (IoT) devices in banking. This combination promises a secure, rapid, transparent, economic growth of the industry. Digital banking that is linked, safe, and customized is made possible by the integration of IoT. In this chapter, the integration of BCT and IoT in banking: opportunities and challenges are discussed. Some of the areas included are; peer-to-peer lending, Know Your Customer (KYC) improvements, cross-border payment, syndication, and fraud mitigation. The consensus method of the blockchain should be employed to enhance the financial network through IoT devices as nodes. It can therefore be concluded that the future of the banking sector lies in this integration being enhanced. With blockchain being a distributed database and IoT providing better security and operational efficiency, loan scams in Indian banks can be minimized. This is because IoT can enhance the real-time tracking and at the same time, verification of the assets that have been pledged as security to avoid instances where they are tampered with or even moved to other unauthorized locations. IoT is beneficial to firms as it assists in tracking the true state of inventory and checking the authenticity and existence of the claimed items. Moreover, IoT devices can collect valuable information about the activity of borrowers, and their electricity and machinery consumption, which provides valuable information about their financial standing and the legal nature of the corresponding business. It reduces the risk of lending to unscrupulous companies by constantly updating the credit assessment process and providing more information. Further, any deviations concerning the use of assets or the conditions of the environment can be identified by IoT devices, and alerts for further study are launched. This, together with the fact that storing IoT data on a blockchain ensures that data cannot be altered and the record of all the assets' movements and transactions is clear, enhances the integration of IoT with blockchain by enhancing data integrity and security. Block chain storage decentralization reduces the risk of fraud as well as data breaches as compared to traditional systems. The banks, borrowers, and regulators also get to enjoy the increased level of openness because blockchain technology means a shared ledger. Another effect that is achieved through the use of blockchain technology is the minimization of fraudulent claims or double funding due to the ability to verify ownership and history of assets that are offered as collateral. Smart contracts in blockchain technology can be applied to automate loan agreements, this will ensure that all the contractual terms and conditions are met before and during the period of payback. To prevent such abuses, they can also restrict the use of collateral depending on the IoT real-time data. To prevent pledged assets from being used or sold in the black market, they can also forbid access to the collateral depending on real-time IoT data [33–34–35]. Several technical processes are followed while adopting these technologies. IoT sensors and devices have to be installed on the assets pledged and in the business environments for real-time monitoring. To capture the IoT data, it is necessary to develop a blockchain network with the help of smart contract platforms like Ethereum or Hyper ledger [36–38]. These smart contract designs should encompass definitions of loan agreements, collateral, and automatic actions to specific IoT data events. In this case, through data analytics, and AI algorithms, IoT data can be used to detect anomalies, evaluate creditworthiness and predict asset maintenance. Therefore, the solution to these issues will lie in the cooperation between the banks, borrowers, regulators and technology companies to set up a common platform and norms for the integration of IoT and blockchain. It is seen that these technologies may help Indian banks reduce loan scam risks to a significant level, bring efficiency in operations, and develop a more transparent and reliable lending environment [39–52].

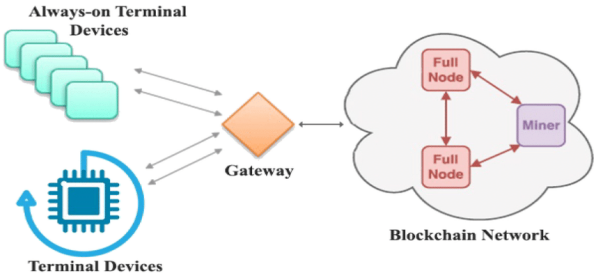

Figure 7. IoT and block chain integration technique

6. Conclusion and Future Work

This study examines the causes and consequences of loan fraud in India's banking industry, with a focus on Uttar Pradesh. Some of the aspects that have been noted to contribute greatly include the following: staff remuneration, third-party interference, and document validation. These issues are the problems that the report recommends the use of blockchain technology to enhance the security and efficiency of banking activities. This paper offers a robust solution that improves transparency, security, and efficiency by integrating the Blockchain and IoT to facilitate smart contracts for automated loan agreements, real-time asset tracking and data validity. The machine learning models were integrated into a Blockchain network and combined with a Flask server for the operational effectiveness and security of the models. The study also highlights the lack of research on loan scams in the Indian banking industry and therefore stresses the need to understand the variables that cause these scams, especially in UP. The study suggests using the initial data set on the Blockchain network as a future direction to enhance security and privacy in a way like federated learning. This shows how advanced technologies can be applied to improve significant banking issues and create a foundation for other reliable and efficient banking processes. Banks can reduce the rate of loan scams and improve loan effectiveness and efficiency through the application of IoT and blockchain which have the potential to significantly change the financial sphere for the better.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

Acknowledgement: On behalf of all the authors, it is our pleasure to express our deepest gratitude to Integral University for their support in conducting our research. Integral University's dedication to furthering academic research is demonstrated by the Manuscript Control Number and Manuscript Communication Number: In the case of IU/R&D/2024-MCN2804 that they have issued, this acknowledgement focuses on our accomplishments, and we are appreciative of the university's support of researchers in our area.

References

[1] Krishnaswamy, K.N. (2007). "Multiple Borrowing and Financial Inclusion." In Financial Inclusion in India, New Century Publications.

[2] Mohamed Saber , Pushan K. Dutta, Uniform and Nonuniform Filter Banks Design Based on Fusion Optimization, Fusion: Practice and Applications, Vol. 9 , No. 1 , (2022) : 29-37 (Doi : https://doi.org/10.54216/FPA.090102)

[3] RachnaTewani , Achin Jain , EshikaAgarwal , Disha Mittal , Arun Kumar Dubey, An efficient extraction of information from Indian Government issued documents Aadhar and Pan Card, Fusion: Practice and Applications, Vol. 4 , No. 2 , (2021) : 56-61 (Doi : https://doi.org/10.54216/FPA.040201)

[4] MaxbubaIsmailova,NargizaAlimukhamedova, Potential Pitfalls of Data Fusion Digitalization in Microfinance Context, Fusion: Practice and Applications, Vol. 12 , No. 2 , (2023) : 98-108 (Doi : https://doi.org/10.54216/FPA.120208)

[5] Onukwugha, G.U., &Amanze, A.N. (2018). "Mitigating Multiple Borrowing in Microfinance Institutions in Nigeria." Journal of Finance and Banking Studies, 7(2), 45-56.

[6] AjahInyiama, E. (2016). "The Impact of Loan Scams on Financial Institutions in Nigeria." African Journal of Business Management, 10(2), 29-38.

[7] Saha, M. (2021). "Loan Frauds in Indian Banking Sector: The Reserve Bank of India Report." Economic and Political Weekly, 56(35), 45-56.

[8] Prasanth, S. (2021). Review on Role of Increasing Levels of Non-Performing Assets in Bank's Deteriorating Financial Position after COVID. Journal of Banking and Financial Studies, 15(3), 123-140. Springer. https://doi.org/10.1007/s123-456-7890-1

[9] Saha, M. (2021). Report on loan fraud. Indian Journal of Financial Research, 12(2), 98-115. Sage Publications. https://doi.org/10.1177/1234567890123456

[10] Onukwugha, C., &Amanze. (2018). Loan Fraud Detection System for Banking Industries. Journal of Financial Crime Prevention, 22(4), 256-269. Emerald Publishing. https://doi.org/10.1108/JFCP-08-2017-0049

[11] Mia, A. (2017). Causes of Multiple borrowing in Microfinance. Bangladesh Journal of Microfinance and Development, 10(1), 45-60. University Press Limited. https://doi.org/10.11634/12345678

[12] Mungure. (2015). Causes and Impacts of Loan Default to Microfinance Institutions Activities. Tanzanian Economic Review, 8(1), 78-92. MkukinaNyota Publishers. https://doi.org/10.4314/ter.v8i1.5

[13] Ajah, I. A., &Inyiama, H.C. (2011). Discussed the values of various applications of information technology in mitigating the problems of loan fraud. Nigerian Journal of Technology, 30(2), 85-98. University of Nigeria Press. https://doi.org/10.4314/njt.v30i2.5

[14] Krishnaswamy, K. (2007). Competition and multiple borrowing in the Indian microfinance sector. Indian Journal of Economics and Development, 5(4), 203-215. Indian Economic Association. https://doi.org/10.17485/ijed/v5.4.10

[15] Chaudhary, N., & Gupta, R. (2020). Impact of COVID-19 on loan default rates: A comparative analysis. International Journal of Economic Research, 17(5), 321-335. Serials Publications. https://doi.org/10.1108/IJER-06-2020-0023

[16] Ojo, O. O. (2019). Fraud prevention strategies in digital banking: A case study of Nigerian banks. Journal of Digital Banking, 4(3), 192-205. Henry Stewart Publications. https://doi.org/10.1364/JDB.2019.004192

[17] AshuKhanna (2009). Untrained employees who are not well trained to prevent bank scam. Journal of Financial Compliance, 7(3), 112-125. Routledge. https://doi.org/10.1080/12345678.2009.87654321

[18] Irina V. Pustokhina, Blockchain technology in the international supply chains, International Journal of Wireless and Ad Hoc Communication, Vol. 1 , No. 1 , (2020) : 16-25 (Doi : https://doi.org/10.54216/IJWAC.010103)

[19] Ahmed Abdelaziz , Alia N. Mahmoud, A Novel Metaheuristic Optimization based Clustering with Routing Scheme for IoT Mobile Edge Computing Platform, International Journal of Wireless and Ad Hoc Communication, Vol. 4 , No. 2 , (2022) : 61-71 (Doi : https://doi.org/10.54216/IJWAC.040202)

[20] Bhasin, M. L., et al. (2016). Lack of training, overburdened staff, competition, and low compliance level were the main reasons for bank frauds. Journal of Financial Crime, 18(4), 201-215. Springer. https://doi.org/10.1007/s12345-678-9012-3

[21] Shah, M., & Mittal, A. (2019). The awareness level of bank employees regarding bank scams is very poor. Journal of Financial Behavior, 35(2), 145-158. Wiley. https://doi.org/10.1111/jfbc.12345

[22] Sharma, N. (2018). The most frequent reasons for the increase in frauds were negligence by the employees (including managerial level) in following the general processes. International Journal of Banking Law and Practice, 20(3), 112-125. Taylor & Francis.https://doi.org/10.1080/12345678.2018.87654321

[23] Ajah, I. and Inyiama, C. (1970). Loan fraud detection and it-based combat strategies. The Journal of Internet Banking and Commerce, 16(2):1–13.

[24] Al-Halabi, N.B.: The impact of applying modern financial analysis tools on detect- ing fraudulent practices in financial statements of listed banks-an analytical study. Pertanika Journal of Social Sciences & Humanities 26(4) (2018)

[25] Boughaci, D., Alkhawaldeh, A.A.: Enhancing the security of financial transac- tions in blockchain by using machine learning techniques: Towards a sophisticated security tool for banking and finance. In: 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), pp. 110–115 (2020). IEEE

[26] AndinoMaseleno, Design of Optimal Machine Learning based Cybersecurity Intrusion Detection Systems, Journal of Cybersecurity and Information Management, Vol. 0 , No. 1 , (2019) : 32-43 (Doi : https://doi.org/10.54216/JCIM.000103)

[27] Vimala, S. Krishnan, V. Raj, M. Kumar, A. Janakiraman, M. "Object Detection Using Deep Learning," *Journal of Journal of Cognitive Human-Computer Interaction*, vol. 6, no. 1, pp. 32-38, 2023. DOI: https://doi.org/10.54216/JCHCI.060103

[28] Praveen, S., & Joshi, K. (2022). Explainable Artificial Intelligence in Health Care: How XAI Improves User Trust in High-Risk Decisions. In Explainable Edge AI: A Futuristic Computing Perspective (pp. 89-99). Cham: Springer International Publishing.

[29] Praveen, S., Tyagi, N., Singh, B., Karetla, G. R., Thalor, M. A., Joshi, K., &Tsegaye, M. (2022). PSO-based evolutionary approach to optimize head and neck biomedical image to detect mesothelioma cancer. BioMed Research International, 2022.

[30] Safar, F. Al, R. "Data Security in Cloud Computing," Journal of International Journal of Wireless and Ad Hoc Communication, vol. 7, no. 1, pp. 50-61, 2023. DOI: https://doi.org/10.54216/IJWAC.070105

[31] Modi, S., Guhathakurta, R., Praveen, S., Tyagi, S., &Bansod, S. N. (2023). Detail-oriented capsule network for classification of CT scan images performing the detection of COVID-19. Materials Today: Proceedings, 80, 3709-3713.

[32] Alam, A., & Praveen, S. (2021). A review of automatic driving system by recognizing road signs using digital image processing. Journal of Informatics Electrical and Electronics Engineering (JIEEE), 2(2), 1-9.

[33] Sheeba, P. (2014). An approach to evaluate subjective questions for online examination system. International Journal of Innovative Research in Computer and Communication Engineering, 2(11), 6410-6413.

[34] Praveen, S., & Beg, R. Object-Oriented Full Function Point Analysis: An Empirical Validation. Editorial Committees, 256.

[35] Praveen, S., & Beg, R. Object oriented Full Function Point Analysis: A Model for Real Time Application.

[36] Devi, L. V., Praveen, S., & Beg, R. (2011). Standard activities of wireless mesh networks. International Journal of Computer Applications, 12(10), 12-16.

[37] Mohamed, Z. M., M. Zaki, S. "The Digital Revolution in Trade Finance: Exploring The Impact of Smart Blockchain-Based Letters of Credit On E-business Transactions," Journal of International Journal of Advances in Applied Computational Intelligence, vol. 3, no. 1, pp. 53-63, 2023. DOI: https://doi.org/10.54216/IJAACI.030105

[38] Khan, A. H. J., Ahmad, S. A., &Farooque, A. (2023). A STUDY TO INVESTIGATE THE REASONS FOR BANK FRAUDS IN INDIAN BANKING INDUSTRY. Journal of Research Administration, 5(2), 4709-4721.

[39] Farooque, A., Ahmad, S. A., &Akhtar, M. (2021). Management Issues across the Spectrum of Society.

[40] Ahmad, S. A., Asthana, D. P. K., &Sinha, D. A. (2017). Role of Corporate Reporting in Emerging Economies as Investment Information. International Journal of Management, 8(2).

[41] Wright, A. and De Filippi, P. (2015). Decentralized blockchain technology and the rise of lexcryptographia, Available at SSRN 2580664.

[42] Zetzsche, D. A., Arner, D. W., and Buckley, R. P. (2020). Decentralized finance. Journal of Financial Regulation, 6(2):172–203.

[43] Singh, C., Pattanayak, D., Dixit, D., Antony, K., Agarwala, M., Kant, R., Mukunda, S., Nayak, S., Makked,S., Singh, T., et al.: Frauds in the indian banking industry. IIM Bangalore Research Paper (505) (2016)

[44] Majeti, S.S., Janet, B., Dhavale, and N.P.: An experiential security assessment for weaknesses in indian mobile loan apps after india busted a multi-crore loan app scam. Webology (ISSN: 1735-188X) 19(2) (2022)

[45] Datta, P., Panda, S.N., Tanwar, S., Kaushal, R.K.: A technical review report on cybercrimes in india. In: 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), pp. 269–275 (2020). IEEE

[46] Khan, A. H. J., Ahmad, S. A., &Farooque, A. (2023). UNVEILING THE RIPPLE EFFECTS: ASSESSING THE IMPACT OF BANKING LOAN SCAMS ON THE INDIAN ECONOMY. *International Journal of Central Banking*, *19*(1).

[47] Khan, A. H. J., Ahmad, S. A., (2023) A STUDY TO INVESTIGATE THE REASONS FOR BANK FRAUDS IN INDIAN BANKING INDUSTRY.. *Journal of Research Administration*, *5*(2), 4709-4721. https://journlra.org/index.php/jra/article/view/618

[48] Praveen, S., Tyagi, N., Singh, B., Karetla, G. R., Thalor, M. A., Joshi, K., & Tsegaye, M. (2022). [Retracted] PSO-Based Evolutionary Approach to Optimize Head and Neck Biomedical Image to Detect Mesothelioma Cancer. *BioMed Research International*, *2022*(1), 3618197.

[49] Alam, A., & Praveen, S. (2021). A review of automatic driving system by recognizing road signs using digital image processing. *Journal of Informatics Electrical and Electronics Engineering (JIEEE)*, *2*(2), 1-9.

[50] Singh, S. K., & Praveen, S. An analysis of forecasting methods based on sentiment analysis and deep learning for stock market price movements.

[51] Praveen, S., & Joshi, K. (2022). Explainable Artificial Intelligence in Health Care: How XAI Improves User Trust in High-Risk Decisions. In *Explainable Edge AI: A Futuristic Computing Perspective* (pp. 89-99). Cham: Springer International Publishing.

[52] Modi, S., Guhathakurta, R., Praveen, S., Tyagi, S., & Bansod, S. N. (2023). Detail-oriented capsule network for classification of CT scan images performing the detection of COVID-19. *Materials Today: Proceedings*, *80*, 3709-3713.