ZKG INTERNATIONAL

ISSN: 2366-1313

Block chain and Artificial Intelligence: Fraud Detection in Banking Sectors

[1]Eadara Anudeep Satya Sai, [2]Mr. M. Srikant Sagar

[1]PG Scholar, Dept of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, TS, India
eadaradeepu74@gmail.com

[2]Assistant professor, Dept of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, TS, India
srikanthsagar20@mgit.ac.in

ABSTRACT

Block chain and artificial intelligence (AI) are two emerging technologies that have the potential to revolutionize how banks detect fraud. Banks can detect and prevent fraudulent activities more efficiently and effectively by combining block chain's secure and immutable record with AI's powerful analytical abilities. This article examines the benefits and drawbacks of combining block chain with artificial intelligence for fraud detection in the banking industry, as well as a full description of recent research in this topic. This paper examines how these technologies might be integrated into existing fraud detection systems and speculates on their future development and utilization. Finally, our research highlights the intriguing potential of block chain and AI for fraud detection in the banking business, as well as the importance of further research and development in this subject.

Keywords: artificial intelligence; fraudulent banking operations; machine learning; fraud detection

I. INTRODUCTION

Banks and financial organizations face a host of fraud-related issues in today's atmosphere. Identity theft, credit card fraud, and money laundering are all instances of fraudulent behaviors that can result in severe financial losses for banks and their customers. The banking industry is constantly looking for innovative ways to prevent fraud, and block chain and artificial intelligence (AI) are two technologies that have the potential to have a significant impact in this field. A distributed ledger, block chain technology enables safe and transparent transactions. In a block chain system, all transactions are recorded in blocks that are linked together to form a chain. Each block contains a digital signature that has been encrypted and protected, a timestamp, and transaction data. Because of its decentralized character, block chain provides a tamper-proof and transparent system that can prevent fraud in financial transactions. AI is a technology that enables computers to learn from data and make decisions based on that learning. AI systems are capable of analyzing vast amounts of data and detecting trends that may signal fraud. By studying prior transaction data, AI can learn to detect aberrant patterns of behavior that may signal fraudulent activity. Block chain technology and artificial intelligence (AI) could be used in tandem to detect and prevent fraud in the banking industry. By merging these technologies, banks may create a system that is both safe and intelligent.

As fraud becomes more sophisticated, we must find new strategies to protect ourselves in this work. The five most frequent strategies of preventing bank fraud are as follows: artificial intelligence, biometric data, consortium data, high technology standards, and machine learning [2].

Following the onset of the COVID-19 pandemic and the war in Ukraine, fraudulent bank transactions have become even more widespread as a result of the considerable shift toward online transactions and the establishment of several charitable funds that criminals employ to fool users.

The purpose of this research was to employ machine learning models to detect fraudulent banking transactions. The study sought to create algorithms capable of reliably recognizing such transactions. Preprocessing techniques and machine learning algorithms were applied. The importance of this work stems from the proposed method's ability to increase the identification of fraudulent banking transactions, particularly during the pandemic when many transactions have switched online and during times of war when numerous organizations and events are collecting money.

In such a system, transaction data would be stored on a block chain, providing a tamper-proof and transparent record of all transactions. AI systems may be trained to analyze transaction data and detect unexpected patterns. For example, artificial intelligence (AI) may monitor a customer's purchasing history and highlight any unusual transactions that depart from the customer's normal spending habits. When a transaction is flagged as suspicious, the block chain may reveal further information about it, such as the source of funds, the individuals involved, and the time and date of the transaction. This information may aid investigators in quickly and accurately tracing the source of the fraudulent conduct.

Implementing AI technology to detect fraudulent banking processes presents various obstacles, including a lack of openness and interpretability in the algorithms used. The complexities of these algorithms can be difficult to grasp at times, making error detection and correction difficult. Furthermore, the use of AI in fraud detection creates important privacy concerns, as personal data is subject to examination and utilization in the decision-making process. These issues must be carefully considered in order to enable the safe and accurate implementation of AI-powered fraud detection systems. The creation of AI-based applications for the recognition of fraudulent banking operations is an active area of research and development, with tremendous potential to increase the efficiency and accuracy of fraud detection. Addressing the obstacles and concerns connected with employing AI in fraud detection, on the other hand, is critical to ensuring its effectiveness and ethical use in the banking industry.

Study limitations in the financial field Artificial intelligence studies to detect bank fraud are beneficial. It is crucial to highlight, however, that this study solely focuses on identifying fraudulent transactions in online banking, whereas other types of financial fraud may necessitate alternative detection approaches. Furthermore, the study's reliability and generalizability may be hampered by the study's small sample size in the financial field. Data availability is particularly important since high-quality data is required to train and test machine learning algorithms. Incomplete and insufficiently diversified datasets can affect the model's accuracy, resulting in false positives in real-world circumstances. Another issue is the possibility of human biases in data selection and analysis, which might affect the method's validity and dependability. It is also critical to prevent overfitting, which occurs when a model performs well on the training dataset but badly on the test dataset due to complexity and limited generalizability.

II. MATERIALS AND METHODS

In order to achieve the objectives described in this study, classification algorithms were used in this work. These algorithms employ features to determine an object's class. To categorize fresh observations, machine learning relies on labeled training data. These algorithms must first examine a dataset of instances with features and related classifications in order to make reliable predictions for future observations. Because they transfer input variables (x) to discrete output functions (y) that reflect categories rather than numerical values, they are classified as supervised learning techniques. The output of categorization algorithms is discrete rather than continuous. The classification algorithm learns from labeled input data, where each input has an associated output.

Classification algorithms are often used to forecast the output for categorical data since their purpose is to limit the category of a given dataset. According to the information in the preceding paragraph, training any classification model requires a data set that demonstrates the relationship between particular feature sets of an object and its class or category. This is why, in order to fit our classification model to the specified job, we selected to use the Credit Card Fraud Detection dataset from the Kaggle platform. For each algorithm and technique, the platform gives the ROC graph curve and AUC metric. For other implementations, a similar set of metrics is supplied. It is also simple to run the program using the Kaggle platform (which was used to develop this software solution), which supports running Jupyter notebooks by default. To begin, the "Run all" button was selected to resume the sequential execution of all commands. Another option is to use any software that supports Jupyter notebooks. The concrete software implementation was saved as a notebook on the Kaggle site and began with the Pandas library loading a dataset. The research workflow is depicted in Figure 1. Figure 1 depicts the stages of a high-level method for a machine learning program solution, including dataset selection and loading, feature standardization, random under sampling, model fitting, model testing, and output of the best model."

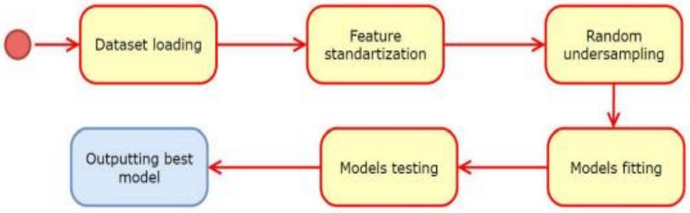


Fig. 1 Scheme of the program solution to the problem

- Choosing a dataset from the Kaggle datasets.
- Loading the dataset into the program (loading the dataset into the program with a library such as pandas or NumPy).
- Using a library like as scikit-learn, divide the dataset into training and testing sets.
- Using a common scaler, standardize the features in the training and testing sets.
- Imbalanced learning, in which the majority class in the training set is randomly under sampled to balance the class distribution.

This algorithm provides a framework for developing a machine learning program solution, including dataset loading, feature standardization, random under sampling, model fitting, model testing, and output of the best model.

Several mathematical elements are used in the described method:

- Algorithms for machine learning,
- Evaluation metrics,

- Data pretreatment techniques.

III. SYSTEM ARCHITECTURE

The architectural design method involves the development of a user registration framework as well as an attacker module to verify the data security of blocks. The goal of the architectural design, as shown in Figure 2, is to enable real-time security analysis.

A. Implementation Methodology

The strategy of integrating block chain and artificial intelligence (AI) for fraud detection in the banking sector generally includes the following phases:

- Recognize the various types of fraud that can occur in the banking business, such as money laundering, identity theft, and payment fraud.
- Look for trends and abnormalities in data sources that are easily available, such as transaction history, customer data, and external data feeds that may indicate fraudulent activities.

Layers needed to construct a block chain:

There are several layers of using block chain and artificial intelligence (AI) for fraud detection in the banking industry. Here are a couple such examples:

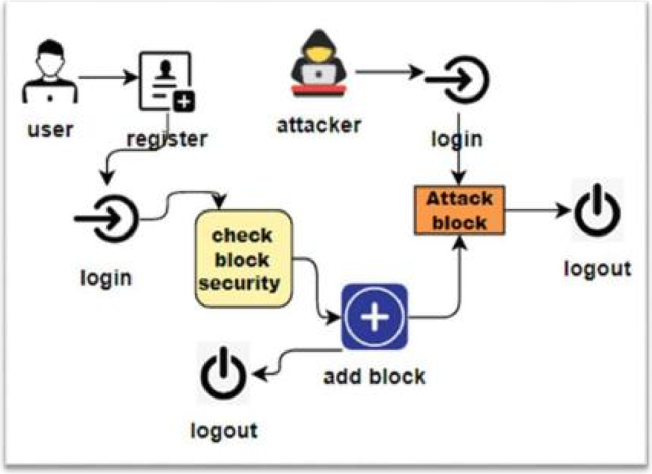


Fig. 2: Block chain and Artificial Intelligence System Architecture for Fraud Detection in the Banking Sector.

- Data Layer: This layer gathers, stores, and processes data from various sources such as transaction history, customer data, and external data feeds.
- Block chain Layer: Implementing a block chain architecture to ensure data security, immutability, and transparency. At this layer, smart contracts can be utilized to automate fraud detection methods and promote safe transactions.
- Artificial Intelligence Layer: Various AI approaches such as machine learning, natural language processing, and data analytics are employed in this layer to analyze obtained data and identify trends that may indicate fraudulent behavior.
- Application Layer: This layer is responsible for the creation of user interfaces and apps that provide banking workers and consumers with insights into fraudulent activity and aid in the detection and prevention of fraud.
- Security Layer: This layer includes implementing security measures to ensure the confidentiality, integrity, and availability of data, as well as preventing unauthorized access and data breaches. These layers work together to provide a comprehensive and effective solution for detecting banking fraud, and they may be changed and improved to fit the specific demands and requirements of every bank or financial institution.

B. Design Methodology

This work has two important components: block chain and artificial intelligence. The block chain component includes smart contracts, transaction verification, cryptography, and consensus procedures. The artificial intelligence component includes fraud detection and data analytics using machine learning. The smart contract is a self-executing contract in which the buyer-seller agreement requirements are directly encoded into lines of code. It facilitates in the automation of certain processes and ensures that all parties involved in a transaction carry out their responsibilities. The transaction verification component ensures that all block chain transactions are legitimate and allowable, preventing fraudulent conduct.

Cryptography and consensus mechanisms are used to protect the block chain and prevent unauthorized access or changes to the contents. Artificial intelligence, on the other hand, aids in the detection of fraudulent behavior through the analysis of transaction data and trends using data analytics and machine learning. The fraud detection component uses machine learning techniques to detect fraudulent actions and sends notifications to the necessary parties.

C. Case Diagram:

In this work, our use case diagram includes three major players: fraud detection, transaction verification, and smart contracts. These participants work in three subsystems: data analytics block chain management, and cryptography and consensus.

Using the Artificial Intelligence subsystem, the Fraud Detection actor examines transaction data and detects fraudulent activity. To validate block chain transactions, the Transaction Verification actor works with the Block chain Management subsystem.

The Smart Contract actor uses the Cryptography and Consensus subsystem to protect the block chain and ensure that all parties involved in a transaction fulfill their commitments. The Data Analytics subsystem provides data to the Fraud Detection actor, which detects fraudulent activity.

D. Sequence Diagram

In this work, our sequence diagram includes two crucial players: fraud detection and transaction verification. The Fraud

Detection agent collects and analyzes transaction data before employing artificial intelligence (AI) algorithms to detect fraudulent behavior. The Transaction Verification actor validates block chain transactions and responds with the result of the verification. When the Fraud Detection actor detects suspicious conduct, it notifies the necessary parties. Overall, this sequence diagram demonstrates how the Fraud Detection and Transaction Verification players interact to discover fraud in the banking business by leveraging block chain and artificial intelligence.

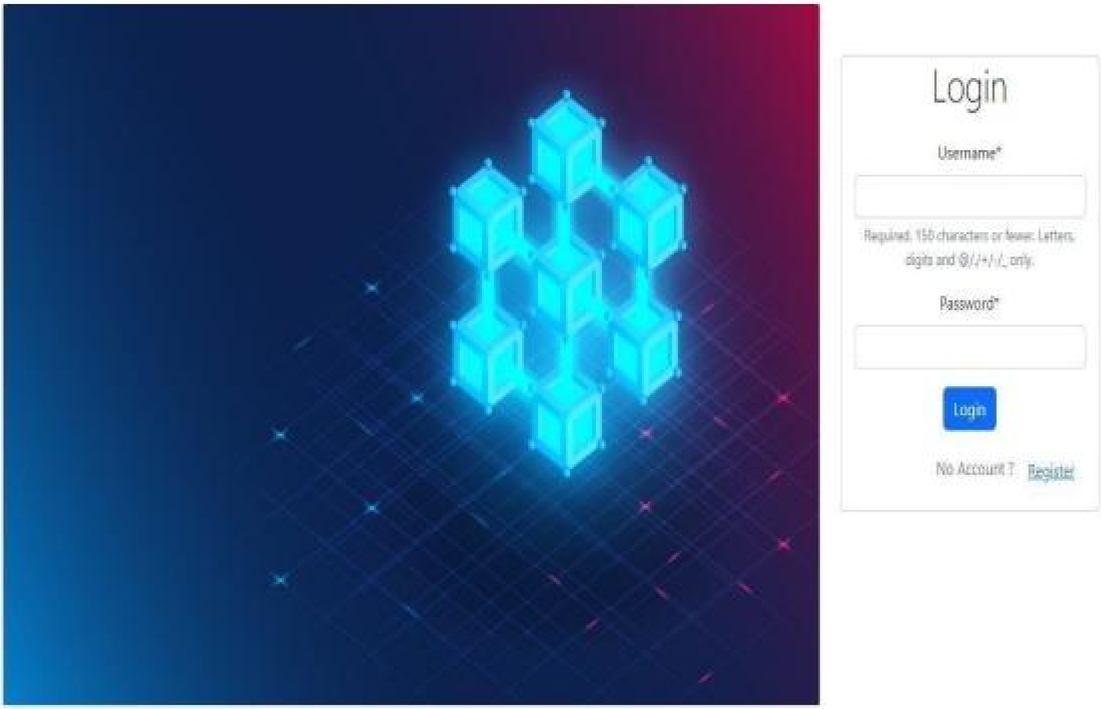
IV RESULTS AND DISCUSSION

The use of block chain and artificial intelligence to detect fraud in the financial industry has yielded promising results.

Banks can use block chain technology to establish a secure and tamper-proof ledger of transactions, making it more difficult for fraudsters to alter data. AI algorithms may then examine the data in real time, flagging any suspicious behavior and prompting bank executives to take action. This technology has the potential to significantly reduce the frequency of fraud in the banking industry, providing greater security and peace of mind to both financial institutions and their clients.

A. *Identity verification:*

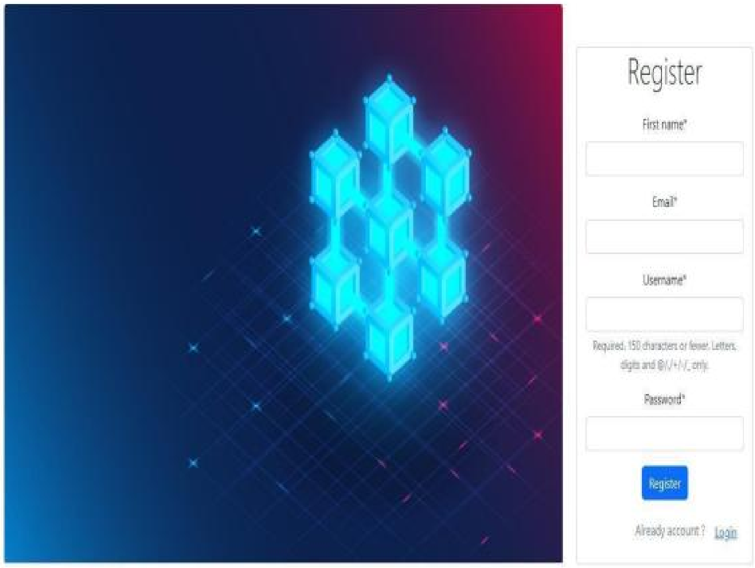
Block chain technology can be used to securely store and verify customer IDs, while artificial intelligence (AI) can be used to analyze consumer activity and identify any unusual trends that may indicate identity theft or fraud. Transaction monitoring: A block chain can provide a secure and transparent record of all transactions, and artificial intelligence (AI) can be used to analyze this data to identify any unusual trends or transactions that may indicate fraud. Risk assessment: Artificial intelligence (AI) may be used to evaluate massive amounts of data in order to discover potential threats and flaws in the financial system, while block chain can be used to securely transmit this information among multiple companies and stakeholders.



Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

Fig. 3 Block chain and Artificial Intelligence Login Page for Fraud Detection in the Banking Sector

ii. When you join up for a block chain and AI-based fraud detection platform in the financial industry, you will typically be asked to provide some basic information, such as your name, email address, and password. Additional information, such as your job title, company name, and industry sector, may be required. In order to ensure that you are a legitimate user, you may be required to go through a verification step in addition to providing basic information.

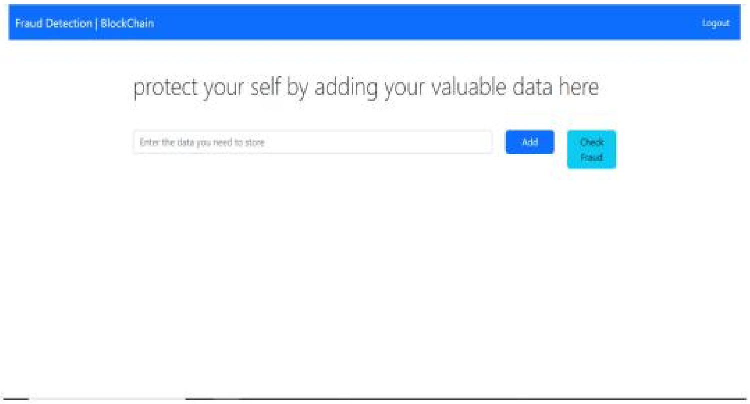


Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

Fig.4 Block chain with Artificial Intelligence User Registration for Fraud Detection in the Banking Sectors

This may entail providing additional evidence, such as a government-issued ID, or submitting to a background check. Following registration and validation, you will typically be provided access to the platform's features and tools for detecting and preventing financial fraud. Real-time transaction and customer behavior monitoring, risk assessment and management tools, as well as advanced analytics and reporting capabilities, might all be included.

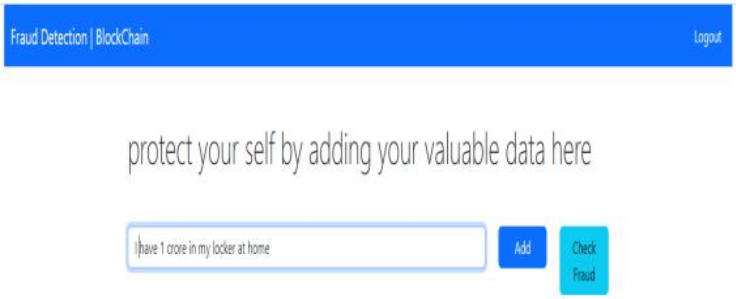
iii. After authentication, the home page is displayed, allowing the user to select an option.


Fraud Detection | BlockChain
Logout
Enter the data you need to store
Add
Check Fraud

protect your self by adding your valuable data here

Fig. 5 Block chain Security Authentication, Fraud Checking and Artificial Intelligence for Fraud Detection in Banking Sector.

iv. The user includes vital information or authentication questions about themselves.

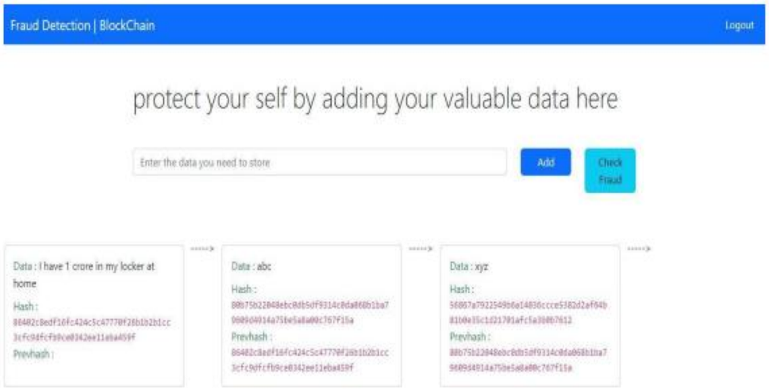


protect your self by adding your valuable data here

I have 1 crore in my locker at home

Fig. 6 Adding Authentication Question for Block chain and Artificial Intelligence in the Banking Sector

v. Individual block display by adding information to authenticated user as information or data or as security questions in which it holds the user's or organization's unrevealing content.



protect your self by adding your valuable data here

Enter the data you need to store

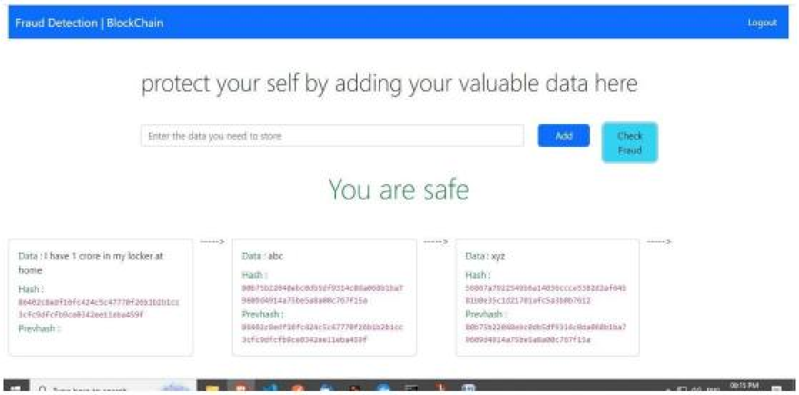
Data : I have 1 crore in my locker at home
Hash : 86482c8edf16fc424c5c47770f26b1b2b1cc3cfc9dfcfb9ce0342ee11eba459f
Prevhash :

Data : abc
Hash : 80b75b22048ebc0db5df9314c0da060b1ba79609d4914a75be5a8a00c767f15a
Prevhash : 86482c8edf16fc424c5c47770f26b1b2b1cc3cfc9dfcfb9ce0342ee11eba459f

Data : xyz
Hash : 56867a7922549b6a14836ccce5382d2af64b81b0e35c1d21701afc5a300b7612
Prevhash : 80b75b22048ebc0db5df9314c0da060b1ba79609d4914a75be5a8a00c767f15a

Fig. 7 Successful Authentication and Display for Information Insertion to Block and representation of the hash and previous hash of each block.

vi. Real-time transaction monitoring: Block chain and artificial intelligence can be used to monitor transactions in real-time, looking for odd or suspicious activity. AI systems may search transaction data for trends or anomalies that could indicate fraud.



protect your self by adding your valuable data here

Enter the data you need to store

You are safe

Data : I have 1 crore in my locker at home
Hash : 86482c8edf16fc424c5c47770f26b1b2b1cc3cfc9dfcfb9ce0342ee11eba459f
Prevhash :

Data : abc
Hash : 80b75b22048ebc0db5df9314c0da060b1ba79609d4914a75be5a8a00c767f15a
Prevhash : 86482c8edf16fc424c5c47770f26b1b2b1cc3cfc9dfcfb9ce0342ee11eba459f

Data : xyz
Hash : 56867a7922549b6a14836ccce5382d2af64b81b0e35c1d21701afc5a300b7612
Prevhash : 80b75b22048ebc0db5df9314c0da060b1ba79609d4914a75be5a8a00c767f15a

Fig. 8 Checking for Fraud in Block chain and Using Artificial Intelligence to Detect Fraud in the Banking Sector

vii. The attacker's home page, where it immediately strikes the blocks.

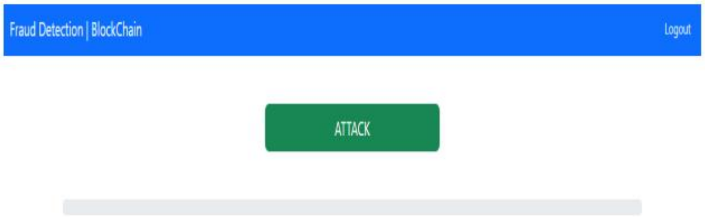
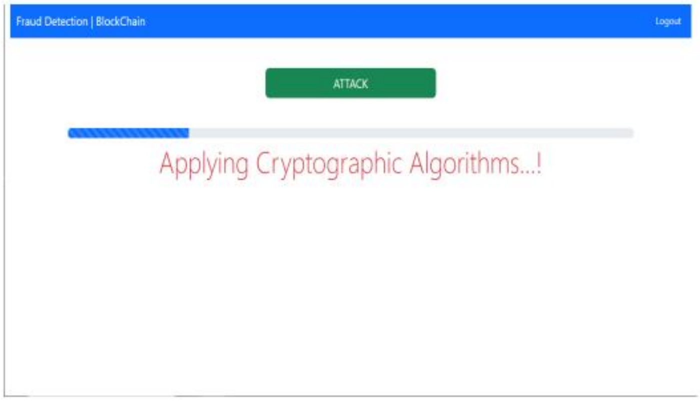


Fig.9 Attacker Home Page for Block chain and Artificial Intelligence for Banking Fraud Detection.

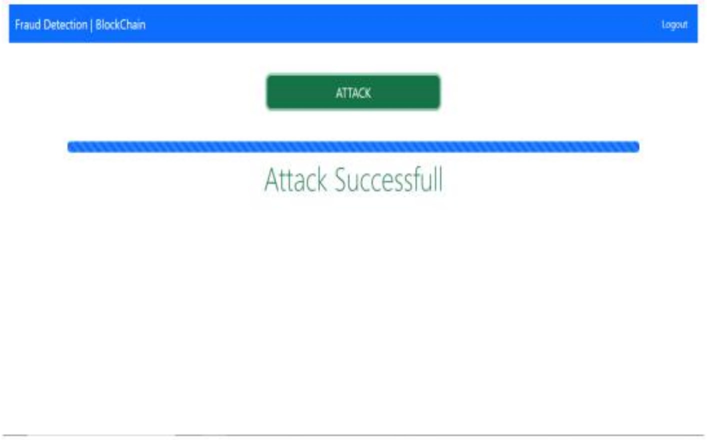
viii. By selecting 'Attack,' a cryptographic approach identical to the SHA-256 algorithm used to construct the block chain is used, allowing you to attack each block separately.



Applying Cryptographic Algorithms...!

Fig. 10 Applying Cryptographic algorithms attack blocks.

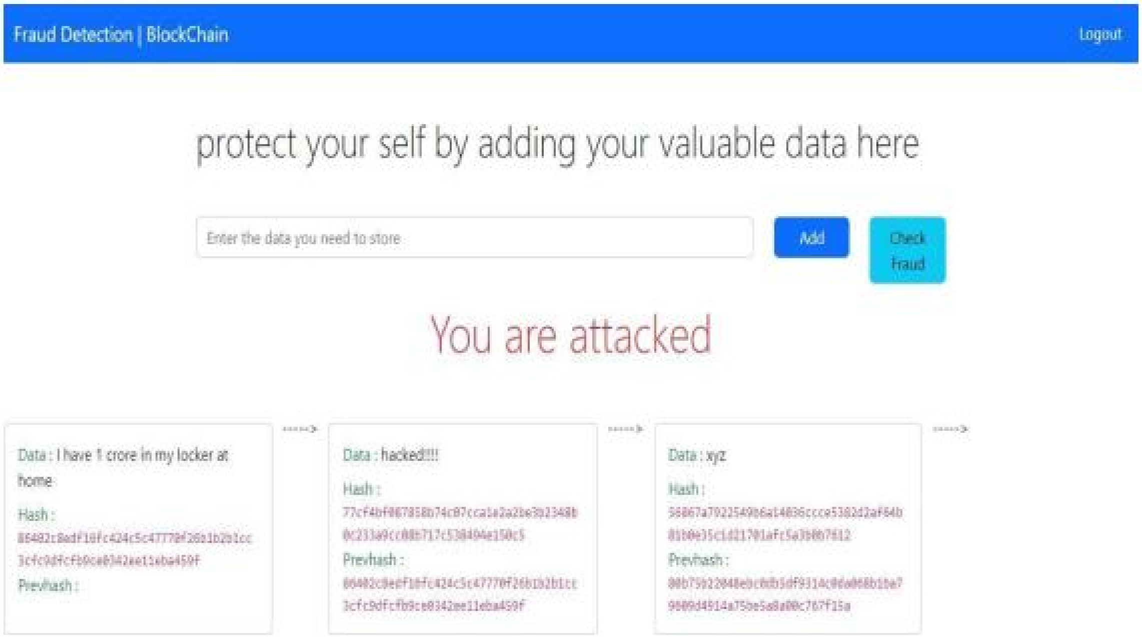
ix. It depicts a successful block attack after the encryption .. algorithm application is finished.



Attack Successfull

Fig. 11 Successful over-the-block assault

x. On the user login page, a real-time notification indicating an attack on the data blocks occurs. As a result, it helps to prevent block updates or fraud.



Fraud Detection | BlockChain

Logout

protect your self by adding your valuable data here

Enter the data you need to store

Add

Check Fraud

You are attacked

Data : I have 1 crore in my locker at home

Hash : 86402c8edf10fc424c5c47770f26b1b2b1cc3cfc9dfcfb9ce0342ee11eba459f

Prevhash :

Data : hacked!!!!

Hash : 77cf4bf087858b74c87cca1a2a2be3b2348b0c233a9cc08b717c538494e150c5

Prevhash : 86402c8edf10fc424c5c47770f26b1b2b1cc3cfc9dfcfb9ce0342ee11eba459f

Data : xyz

Hash : 56867a79225496a14836ccce5382d2af64b81b0e35c1d21701afc5a3b0b7612

Prevhash : 00b75922848ebc0db5df9314c0da068b1be79800d4914a75be5a8a00c767f15a

Fig. 12 Attacked blocks by cryptographic methods, resulting in an alert over the attacked block.

A cryptographic attack is a method for circumventing the security of a cryptographic system by finding a weakness in a code, cipher, cryptographic protocol or key management scheme

V CONCLUSION

Finally, the combination of block chain and artificial intelligence (AI) holds tremendous promise for detecting and combating fraud in the financial industry. Block chain technology provides a secure and transparent platform for storing transaction data, while AI algorithms may analyze the data and discover potentially suspicious patterns of activity. By using this technology, banks can identify and prevent fraudulent transactions more efficiently, minimizing the risk of financial loss and brand damage. The future development of block chain and AI for fraud detection in the banking industry is expected to have a significant impact in a number of areas. They include employing these technologies to improve fraud detection speed and accuracy, risk management and compliance, and customer experience. However, there are concerns about the use of these technologies, such as privacy, data protection, and regulatory compliance. As these technologies evolve, banks must carefully assess the issues and offer effective solutions that are widely accepted by the industry. Finally, the combination of block chain and AI offers the banking industry an exciting opportunity to improve fraud detection and prevention while also offering a more secure and dependable service to their clients.

FUTURE SCOPE

Block chain and artificial intelligence (AI) integration for fraud detection in the banking industry has enormous future potential. As more people use digital banking and financial transactions, the possibility of fraud grows. Block chain and AI provide powerful tools for detecting and preventing fraud, and these technologies are projected to have a significant impact in a variety of industries in the future.

REFERENCE

[1] S. Swain and S. Gochhait, "ABCD technology- AI, Blockchain, Cloud computing, and Data security in the Islamic banking sector," in 2022 International Conference on Sustainable Islamic Business and Finance (SIBF), Sakhir, Bahrain, pp. 58-62, doi: 10.1109/SIBF56821.2022.9939683.

[2] P. Haritha, V. Kavitha, and G. Manimala, "Protection & Privacy Embedding Block chain Established Fraud Detection," in 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, pp. 1437-1444, doi: 10.1109/ICAAIC53929.2022.9792962.

[3] G. D. Reddy, S. Saxena, Eliza, K. R. Isabels, G. Rathnakar and U. Turar, "Utilization of AI for Streamlining and Optimizing Credit Decision Process and Security in Banking Sector," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (ISMAC), Dharan, Nepal, 2022, pp. 715-721, doi: 10.1109/I-SMAC55078.2022.9987389.

[4] R. F. Ibrahim, A. Mohammad Elian, and M. Ababneh, "Illicit Account Detection in the Ethereum Block chain Using Machine Learning," Amman, Jordan, 2021 International Conference on Information Technology (ICIT), pp. 488-493, doi: 10.1109/ICIT52682.2021.9491653.

[5] E. Btoush, X. Zhou, R. Gururaian, K. Chan, and X. Tao, "A Survey on Credit Card Fraud Detection Techniques in Banking Industry for Cyber Security," Doha, Qatar, 2021, pp. 1-7, doi: 10.1109/BESC53957.2021.9635559.

[6] V. Ghai and S. S. Kang, "Role of Machine Learning in Credit Card Fraud Detection," in 2021 3rd International Conference on Advances in Computing, Communication Control, and Networking (ICAC3N), Greater Noida, India, pp. 939-943, doi: 10.1109/ICAC3N53548.2021.9725540.

[7] N. Boutaher, A. Elomri, N. Abghour, K. Moussaid, and M. Rida, "A Review of Credit Card Fraud Detection Using Machine Learning Techniques," Marrakesh, Morocco, 2020, pp. 1-5, doi: 10.1109/CloudTech49835.2020.9365916.

[8] R. Rambola, P. Varshney, and P. Vishwakarma, "Data Mining Techniques for Fraud Detection in the Banking Sector," in 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, pp. 1-5, doi: 10.1109/CCAA.2018.8777535.

[9] A. M. Mubarek and E. Adal, "Multilayer perceptron neural network technique for fraud detection," 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 383-387, doi:10.1109/UBMK.2017.8093417.

[10] S. N. John, C. Anele, O. O. Kennedy, F. Olajide, and C. G. Kennedy, "Realtime Fraud Detection in the Banking Sector Using Data Mining Techniques/Algorithm," 2016 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 1186-1191, doi: 10.1109/CSCI.2016.0224.

[11] Y. Kültür and M. U. alayan, "A novel cardholder behavior model for detecting credit card fraud," in 2015 9th International Conference on Application of Information and Communication Technologies (AICT), Rostov on Don, Russia, pp. 148-152, doi: 10.1109/ICAICT.2015.