JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Data Analytics, Privacy Protection, and Fraud Detection Security Using Blockchain And Machine Learning

[1] Anand Dubey, [2] Dr. Siddhartha Choubey
[1] M. Tech Research Scholar, [2] Professor
[1,2] Computer Science Engineering
[1, 2] Shri Shankaracharya Technical Campus Bhilai, India

ABSTRACT: Blockchain technology, a revolutionary distributed ledger system, has the potential to completely transform a range of sectors, including finance, supply chains, healthcare, and more. The decentralized nature of the block chain, however, makes it particularly challenging to identify and stop fraud. This abstract provides a summary of the state-of-the-art in research and technology for fraud detection in systems based on block chain technology. Beginning with some of the most important characteristics of blockchain, the abstract emphasizes its decentralization, transparency, and immutability. These characteristics provide a strong foundation for assuring data security and integrity, but they also pose challenging difficulties for fraud detection and prevention. The next section of the abstract looks at several fraud types that might occur in blockchain systems, such as double-spending, Sybil Identity theft, attacks, 51% attacks, and flaws in smart contracts. The potential effects of each fraud type on the reliability and integrity of blockchain systems are outlined alongside each fraud type. The abstract provides a summary of the current fraud detection methods used on blockchain systems in attempt to allay these worries. These techniques include many different approaches, including forensic analysis, consensus procedures, and machine learning algorithms, anomaly detection, and cryptographic techniques. The benefits and drawbacks of each approach are highlighted to provide a complete understanding of how it might be applied in various contexts. The lecture also addresses current fraud detection studies connected to blockchains. The fusion of blockchain technology with artificial intelligence is one of these tendencies. the development of fraud detection systems that protect user privacy, the utilization of decentralized and federated machine Utilizing data analytics and visualization tools, learning algorithms, and improving detection and investigation The conclusion of the abstract emphasizes the need of continued study and advancement in fraud detection for systems built on blockchain technology. As blockchain adoption increases across industries, it is crucial to increase the security and reliability of these systems by effectively recognizing and preventing fraud. Discussions of current obstacles and future directions for research inspire more exploration in this important area of study.

IndexTerms **-** Data analytics, blockchain technology, anomaly detection, decentralized ledger, machine learning, cryptography methods, privacy preservation, security, and dependability.

1. INTRODUCTION

Businesses have had a lot of anxiety about financial fraud. Even with technological advances, fraud instances are increasing [1]. In all, merchants are predicted to lose $206 billion due to online transaction fraud between 2021 and 2025, according to a recent Juniper Research analysis [2]. Authentic data must be produced in order for fraud detection systems to function properly. However, financial transaction data is rarely available for machine learning research because of the secrecy surrounding financial data, privacy issues, and a lack of organizational coherence [3]. Organizations frequently avoid taking part in collaborative research on financial problems since it would reveal their financial reporting and corporate goals [4]. The majority of systems and services, as well as a considerable amount of data, are controlled by large corporations. [5]. Crowdsourcing is commonly used by researchers from small businesses to gather data; however it is prone to spoofing and frequently produces utterly useless findings [6]. When an ML model is trained only using intra-organizational data, on the other hand, isolated and exclusive intra-organizational solutions frequently get biased towards a certain piece of evidence [7]. As a result, the huge dispersion is frequently inaccurately duplicated in real-world systems. Machine Learning (ML) systems need real-world data to be reliable and accurate. As we've already mentioned, privacy concerns make it challenging to obtain this information. In online usage situations like transaction fraud detection, the conventional batch-trained machine learning techniques are ineffective [8]. E-commerce is one platform that handles a lot of data flow and receives a lot of visitors. A batch-trained offline ML model quickly becomes unusable as a result, necessitating manual updating, which is expensive in terms of compute, time, and usability. Inside a virtual setting [9]. Furthermore, the Ecosystem's (online) recently launched data instances cannot be taken into account by batch-learning approaches. Continuous machine learning is a method that could help with the goal of maintaining the model's updating throughout time, reducing computing costs, and removing human updates [10]. While the model is already being utilized, ML approaches use an incremental machine learning methodology to learn from a data stream [11]. However, for a fraud detection ML model to continuously improve and keep up with evolving fraud tendencies, a steady supply of data is required. This paper uses block chain and smart contract technology to create an iterative ML model that handles privacy issues. [12]. Tiernanm Barry's research offers concrete proof that batch-trained ML models soon lose their accuracy and dependability when used in an internet environment. In contrast, ML models gradually adjust over time to incoming data. He found that incremental online learning outperforms batch learning when it comes to forecasting the next-minute pricing of the three most well-known crypto currencies. Incremental outlier clustering with a block chain may be more efficient, according to Chao Yang's research. And required less money to calculate [13]. Blockchain technology is rapidly being employed to improve system security, and machine learning techniques are exploited for their predictive powers [14]. The framework for collaborative machine learning was developed by Justin D. Harris and Bo Waggoner using both of these technologies (ML and blockchain) [15]. This platform enables on-the-fly cooperative training of a machine learning algorithm by coupling an incentive mechanism with a data handler. However, they failed to take into account important aspects of the distributed and cooperative environment, such as corporate confidentiality, a range of incentives, and unique mining needs [16]. Additionally, in sectors like e-commerce where data includes both customer personal information and business insights, privacy cannot be compromised [17]. Our study proposes a novel privacy-preserving smart contract and blockchain-based solution to these issues. Business that creates, maintains, and updates a fraud detection model here are a few machine learning techniques for fraud detection using blockchain technology:

1.1 Decision Trees: Decision trees are a popular machine learning method for classification jobs. To identify trends and patterns in transaction data that indicate fraudulent behavior, decision trees can be employed. Building automated fraud detection algorithms using decision trees is another option.

1.2 Random Forests: To improve accuracy and reduce over fitting, the ensemble learning method known as random forests combines several decision trees. Random forests are particularly good at handling large datasets and may discover outliers and irregularities in transaction data that might be evidence of fraud.

1.3 Support Vector Machines (SVMs): The support vector machine (SVM) is a powerful machine learning technology that may be used for both classification and regression tasks. SVMs may be used to find transaction data patterns that indicate fraudulent behaviour. SVMs are extremely helpful for managing complex data and may offer very excellent fraud detection models.

1.4 Neural Networks: A neural network is a machine learning technique that simulates the structure and function of the human brain. Intricate patterns in transaction data that can be indicative of fraud can be taught to recognise using neural networks. They can be used for problems involving classification and regression. Using neural networks, it is also feasible to develop extremely precise fraud detection algorithms.

1.5 Clustering Algorithms: May be used to group similar transactions together and identify patterns in transaction data that indicate fraud. Clustering algorithms may also be used to identify outliers and irregularities in transaction data that may be indicators of fraud. It's important to keep in mind that there isn't a single machine learning method that works well for all types of fraud detection in blockchain. The algorithm to adopt will depend on the specific use case and the characteristics of the transaction data under investigation. It could be required to mix many machine learning techniques to achieve the best fraud detection results. Blockchain technology has completely changed how transactions are tracked, saved, and managed. It provides a decentralised, secure platform that allows transactions to be performed without Clustering algorithms may be used to gather comparable transactions and identify patterns in transaction data that suggest fraud. Clustering algorithms may also be used to identify outliers and irregularities in transaction data that may be indicators of fraud. It is important to keep in mind that no one machine learning technique can completely eliminate the need for middlemen. However, this technology is not impervious to fraud and other unethical activities. Fraud detection in blockchain has become a major problem because of the high transaction value and potential for loss or harm. Below is a review of the blockchain fraud detection literature.

2. BACKGROUND AND RELATED WORK

In 2018, Kshetri et al. released "A Survey of Blockchain Security: From Theoretical Models to Empirical Evaluations." This article provides a thorough explanation of the many approaches that have been used as well as the security problems that blockchain technology is attempting to address. It examines the various ways a blockchain may be attacked, as well as how to recognise and thwart them.

Kshetri et al.'s "Blockchain Forensics: A Comprehensive Review" was published in 2019. This paper provides a comprehensive review of the various techniques used in blockchain forensics. It looks at how to spot and prevent fraud in blockchain transactions using network analysis, graph theory, and machine learning methods.

Singh et al. (2020) claim that deep learning is utilised to identify anomalies in blockchain transactions. This study investigates the use of deep learning algorithms to detect anomalies in blockchain transactions. It illustrates how fraud detection accuracy may be improved by using deep learning algorithms to identify fraudulent transactions.

"Fraud detection in blockchain-based systems: A survey" by Abdellatif et al. (2020) - This study analyses the various techniques for fraud detection in blockchain-based systems. It examines the application of machine learning algorithms, cryptography techniques, and consensus processes for fraud detection.

"Blockchain-based fraud detection for the internet of things" by Li et al. (2021) - This study examines the use of blockchain technology for fraud detection within the context of the Internet of Things (IoT). It highlights how blockchain technology may be used to provide an open and transparent platform for IoT transactions and how machine learning algorithms can be used to identify fraudulent conduct in real-time.

These studies emphasise the importance of fraud detection in blockchain technology as well as the many approaches and techniques that may be used to address this problem. Machine learning algorithms and blockchain forensics techniques are being used to identify and prevent fraudulent activity in blockchain transactions. To develop fraud detection systems that are speedier, more precise, and able to keep up with the constantly shifting threat environment, more research is needed.

3. METHODOLOGY

The following is a block diagram for a block chain fraud detection model:

As a result of bitcoin's phenomenal growth, the scientific and corporate communities have begun to concentrate more on the revolutionary technology known as blockchain. Blockchain is a distributed ledger system that uses encryption to protect transactional or data records [17]. In a peer-to-peer network, records of transactions or data are maintained as blocks of data [18]. All following blocks are related to the genesis block, which is the first block [19]. Blockchain's main goal is to maintain transaction records that are decentralised, immutable, transparent, accessible, and secure while also preserving anonymity [18]. Blockchain is a decentralised peer-to-peer network free from centralised control since no single node or set of nodes has exclusive access to the data. Alternatively, the connected nodes are all equally powerful over the network of blockchains [20].

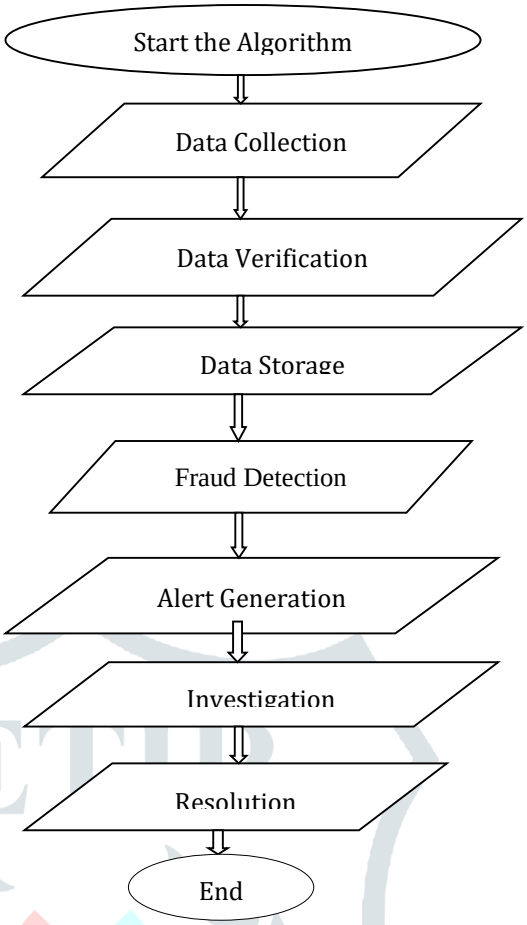

Figure3.1: Design Flow

3.1 Data collection: The first step in the fraud detection process is the gathering of data from various sources, such as user profiles, historical data, and financial transactions. This data is then encrypted and added to the blockchain ledger.

3.2 Dataset Description:

1) The phrase "step-by-step" can be used to describe real-time simulation. One step equals one hour in real time. There are 744 actions total in the collection, distributed over 30 days.

2) There are five different transaction types: cash in, cash out, debit, payment, and transfer.

3) Amount: The transaction's value; Name Original: The sender's name;

4) Identification for the receiver, Name Dest.

5) Old skool Org: The sender's account balance before a transaction

6) After a transaction, the new balance of the sender's account is shown.

7) Old skool The balance of the receiver's account just before a transaction

8) Balance New Dest: The receiver's account balance after a transaction.

9) This feature marks transactions that amount more than $2,000 in a single attempt as fraudulent.

10) Is Fraud: This property, which also functions as the target variable, shows whether or not the transaction is fraudulent.

3.3 Data attestation:

A number of network nodes verify and approve the data before it is posted to the blockchain. The verification process ensures that the data is accurate, trustworthy, and undamaged.

Number of each type of transaction, both legal and illegal.

PAYMENT:
The whole amount, 2151495,
Is Authentic = 2151495
Is Fraud = 0
TRANSFER:
The sum of 532909
Is Lawful = 528812
Is Fraud = 4097
CASH_OUT:
The total amount of 2237500
Is Lawful = 2233384
Is Debit = 4116
For fraud:
Total is 41432
Lawful = 41432
Is Fraud = 0
CASH_IN:
The sum of 1399284
Equals True = 1399284
Is Fraud = 0

3.4 Storage of data:

Once the information has been verified, a block is added to the blockchain record. Each block in the chain contains a unique hash that uniquely identifies it and links it to the block before it, providing an immutable record of all transactions and events.

3.5 Models Selection and Training:

The following are the 5 models that we'll be using from the Scikit-Learn library:

1. BERNOULLI NB
2. MULTINOMIAL NB
3. CLASSIFIER FOR PASSIVE-AGGRESSIVE
4. SGD Classifier
5. PERCEPTRON

3.5.1. Bernoulli NB Model:

The chance of different classes is predicted using a supervised machine learning method called Naive Bayes based on a range of characteristics. It displays the likelihood that an event will take place. Naive Bayes is also known as conditional probability.

Example:

(i) Using the Bernoulli Naive Bayes classifier and the presented data, it is feasible to detect whether a person is unwell or not. This would be a binary classification issue, which would be ideally suited for the Bernoulli Naive Bayes method.

(ii) In text classification, a Bernoulli-Naive Bayes classifier may also be used to determine if an SMS is "spam" or "not spam."

3.5.2. Multinomial NB Modal:

The Multinomial Naive Bayes algorithm is a popular Bayesian learning method in Natural Language Processing (NLP). The application produces an informed guess regarding the tag of a text, such as an email or news story, using the Bayes principle. The tag with the highest likelihood is produced after calculating the likelihood of each tag for a certain sample. The Naive Bayes classifier classifies features that are different from one another, which combines the several methods that make up the classifier. One characteristic's inclusion or exclusion is independent of the existence or absence of another

attribute. The Naive Bayes approach works well for looking at text input and addressing problems involving several classes. The outcome is One must first comprehend the idea of the Bayes theorem in order to fully appreciate the Naive Bayes theorem. Thomas Bayes developed the Bayes theorem, which determines the likelihood of an event occurring based on knowledge of its conditions. When predictor B is available, we calculate the probability of class A. The following formula serves as its basis: P(A|B) = P(A) * P(B|A)/P(B).

3.5.3. Classifier for Passive-Aggressive Modal:

The passive-aggressive classifier (PAC) is a well-liked linear classification method in machine learning for text classification issues. The PAC algorithm belongs to the family of online learning algorithms, which implies that when it is exposed to new data, it gradually learns new information. It is especially well suited for these kinds of applications since data arrives continuously over time in large-scale or streaming applications. The algorithm's modification of its weights or coefficients during training is referred to as "passive-aggressive" behaviour. A linear boundary that separates positive and negative samples is essentially what the PAC algorithm searches for in the feature space. Every time it encounters a new training example, it first creates a prediction using the current weights. The algorithm alters the outcome if the prognosis is right. Weights. The strategy penalises any modifications that go against the margin if the prediction is inaccurate while simultaneously updating the weights in a way that minimises the error. The classifier is ensured by this penalty term to maintain conservatism and refrain from significantly changing the weights unless absolutely necessary. The PAC approach is simple, rapid, and effective for many text classification issues. It presupposes a linear relationship between traits and class labels, therefore datasets with complex or nonlinear decision constraints might not be the best fit.

3.5.4. SGD Classifier:

The SGD Classifier (Stochastic Gradient Descent Classifier) is a type of linear classification method used in machine learning. It belongs to the class of online learning algorithms that gradually changes the weights of its parameters in response to each fresh example it encounters. In disciplines like computer vision and natural language processing, the SGD Classifier is commonly used for complicated and high-dimensional classification problems. Depending on the gradient of the loss function relative to the weights, which is established for each training sample, it updates the weights. As a result, the algorithm can quickly and successfully learn from a massive amount of data. One of the advantages of the SGD Classifier is its capacity to support efficient online learning, which implies that it may learn from as opposed to a static stream of data, a dynamic dataset. It is especially well suited for problems requiring large datasets and high-dimensional feature spaces because of its capacity to scale to enormous datasets and process samples in batches. Like other linear classifiers, the SGD Classifier assumes a linear connection between the features and the target variable, which may not be true for all datasets. The choice of hyperparameters, such as the learning rate and regularisation strength, which need to be properly adjusted for optimum results, also affects how well the SGD Classifier performs.

3.5.5. Perceptron Modal:

The perceptron is a simple and well-liked machine learning method for binary classification tasks. The best hyperplane for partitioning the two classes of data points is found using this specific linear classifier. The Perceptron approach was first proposed by Frank Rosenblatt in 1958, and it is being used today as the basis for more complex models.

3.6 Fraud detection:

Machine learning algorithms are used to examine the blockchain's data in order to seek for patterns and anomalies that might indicate fraud. The analysis can be carried either regularly or in real-time, depending on the requirements of the application.

In [31]:

```
# splitting features and target in different datasets
data=df3.copy()
X=data.select_dtypes(exclude=['object']).drop(columns="isFraud")
Y=data.isFraud
print(X.shape,Y.shape)
```

```
(2770409, 6) (2770409,)
```

In [32]:

```
# Splitting dataset in to training and testing
x_train, x_test, y_train, y_test = train_test_split(X, Y, test_size=0.11, shuffle=True)
print(x_train.shape, x_test.shape, y_train.shape, y_test.shape)
```

```
(2465664, 6) (304745, 6) (2465664,) (304745,)
```

In [33]:

```
# Creating some global variables for future use.
bnb, mnb, pac, sgd, perc = None, None, None, None, None
models={"bnb":bnb, "mnb":mnb, "pac":pac, "sgd":sgd, "perc":perc}
preds, cr = {}, {}
```

3.7 Alert generation:

An alert is created and delivered to the appropriate stakeholders, such as users, financial institutions, or law enforcement authorities, when a suspected fraud is found. The warning contains comprehensive details on the alleged suspicious behaviour, including the sum of the transaction, the location, and the time.

3.8 Investigation:

An investigation is started based on the alert to confirm the suspicious conduct and establish the scope of the scam. Additional data gathering, analysis, and cooperation with other network participants may be required for the inquiry.

3.9 Resolution:

Following the conclusion of the inquiry, the proper steps are taken to address the fraud, such as banning the user account, cancelling the transaction, or bringing legal action against the perpetrator. The resolution is also added as a new block to the blockchain ledger, assuring accountability and transparency. In conclusion, a blockchain-based fraud detection strategy gathers, validates, and stores data in an immutable ledger before utilising machine learning algorithms to detect and stop fraudulent behaviours. The methodology provides openness and accountability in the fraud detection process in addition to guaranteeing the data's security and integrity.

3.10 Set of Data for a Block Chain Fraud Detection Model:

Due to the fact that this subject is still in its infancy and data is not easily available, finding a sufficient dataset for a blockchain model for fraud detection may prove difficult. But there are certain publicly accessible datasets that can be applied to blockchain fraud detection:

3.11 Web of trust dataset for Bitcoin OTC:

Users of the Bitcoin OTC platform's trust connections make up this dataset. Features like user IDs, ratings, and comments are included. It is possible to utilise it to create models for identifying phoney users and transactions.

3.12 Dataset for Bitcoin Alpha:

Transaction information from the Bitcoin blockchain makes up this dataset. It has attributes including timestamps, input and output addresses, transaction amounts, and transaction IDs. It may be utilised to create models for identifying suspicious activity and unusual transactions.

3.13 Bitcoin dataset:

Transaction information from the Ethereum blockchain makes up this dataset. Features including transaction IDs, sender and recipient addresses, transaction amounts, and petrol surcharges are included. It may be used to create models for identifying transaction manipulation and fraudulent smart contract execution.

3.14 Market Statistics and Crypto Currency Prices:

This dataset includes daily market and price data for a number of digital coins, including Bitcoin, Ethereum, Lite coin, and Ripple. It may be used to create models for spotting insider trading and price manipulation. It is crucial to remember that due to their size and scope limitations, these datasets might not be adequate for creating reliable fraud detection algorithms. To increase the precision of the models, it is advised to combine these datasets with additional pertinent data sources such news articles, user behaviour data, and sentiment analysis of social media.

4. RESULTS AND DISCUSSION

Along with the findings from earlier work for this dataset, we now have the following Results after training:

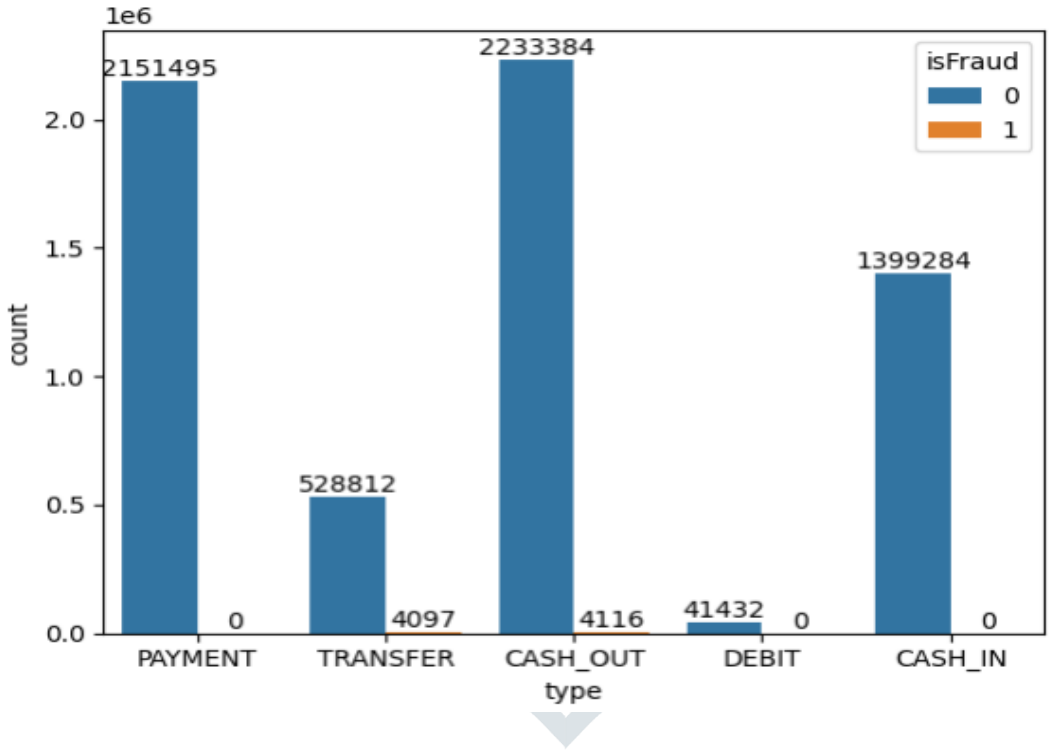

Figure 4.1: Count of legitimate and fraudulent transactions for each type of transaction

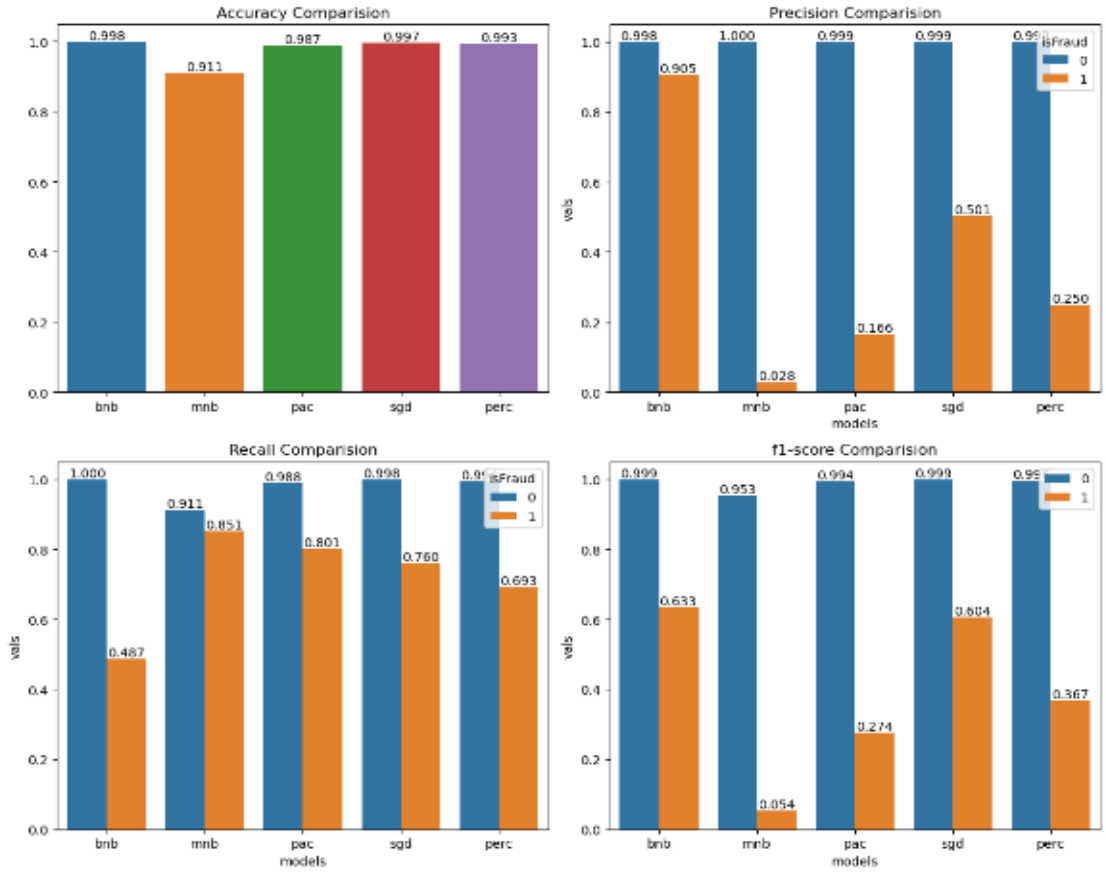

Figure 4.2: All Models' Performance Matrix Graph

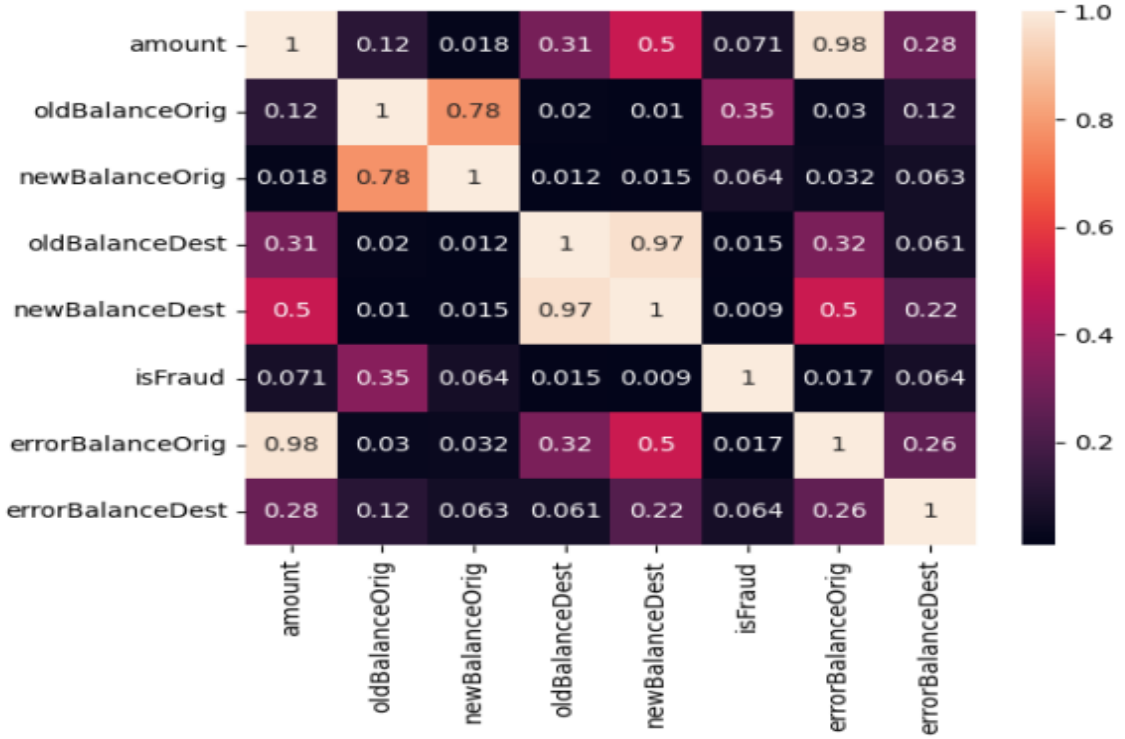

Figure 4.3: Matrix Of Passive-Aggressive Misunderstanding For First Instruction.

ML Model	Training Acc	Testing Acc	Precision		Recall		$F\beta$-Score		False Negative Rate
			0	1	0	1	0	1	
SGD	85.58	86.55	0.99	0.78	0.72	0.99	0.83	0.87	0.059
Perceptron	92.56	92.63	0.94	0.91	0.91	0.92	0.93	0.93	0.058
MNB	80.86	80.73	0.84	0.78	0.76	0.86	0.80	0.82	0.14
BNB	72.70	72.15	0.69	0.77	0.82	0.62	0.75	0.69	0.38
PAC	**93.7**	**93.64**	**0.96**	**0.92**	**0.94**	**0.96**	**0.93**	**0.94**	**0.041**

Table 4.1 Shows Previous Outcomes

ML MODEL	Accuracy	Precision		Recall		Fβ Score	
		0	1	0	1	0	1
SGD MODAL	99.1	0.999	0.227	0.992	0.776	0.995	0.351
PERCEPTRON MODAL	99.1	0.999	0.23	0.991	0.829	0.995	0.36
MNB MODAL	91.2	1	0.031	0.912	0.886	0.954	0.06
BNB MODAL	99.8	0.998	0.913	1	0.513	0.999	0.657
PAC MODAL	**99.8**	**0.999**	**0.808**	**0.999**	**0.681**	**0.999**	**0.739**

Table 4.2: Our Results Table (The Final Score)

We will examine recall for Comparison since we want to be sure to catch the majority of scam transactions.

Therefore, it is clear from above that we are receiving the greatest recall in PAC.

And when compared to their prior findings, their recall for identifying PAC fraud was 96%, whereas ours was 68%.

5. CONCLUSION

In order to improve the security and reliability of decentralized ledger systems, fraud detection in blockchain technology-based systems is an important area of research and development. Blockchain technology provides a solid foundation for data security and integrity because to its distinguishing features including immutability, transparency, and decentralization. However, these characteristics make it challenging to spot and stop fraud. Numerous fraud types, including as double-spending, Sybil attacks, 51% attacks, smart contract problems, and identity theft, pose a severe danger to the reliability and integrity of blockchain systems. To detect and halt such fraudulent activities, it is essential to use effective and robust fraud detection systems. Blockchain systems today incorporate a wide range of techniques, such as anomaly detection, machine learning algorithms, and consensus. Determine fraud. Processes and procedures for forensic analysis and cryptography each approach has pros and cons, and whether it can be applied relies on the specific requirements and circumstances of the blockchain system.

The most recent advancements in fraud detection research pertaining to blockchains offer prospective avenues for more research. Making use of decentralised and federated machine learning approaches, developing privacy-preserving fraud detection mechanisms, and utilising data analytics and visualisation techniques are some of the potential ways to improve fraud detection capabilities. Continuous research and improvement in fraud detection for systems based on blockchain technology is crucial as blockchain usage extends across industries. By effectively recognizing and preventing fraud, these systems may become more dependable and trustworthy, allowing for widespread adoption and use across a range of sectors. But there are still problems with scalability, privacy, and adaptability to evolving fraud tactics. Future study should focus on resolving these issues, exploring novel detection methods, and establishing frameworks and best practices for fraud detection in blockchain systems. In general, the subject of fraud detection in blockchain-based systems is dynamic and necessitates collaboration among different academic fields and continual innovation. Further research in this area may improve the security, dependability, and reliability of blockchain systems, which would promote the creation and adoption of decentralized apps and services in the digital age.

Future work (Scope of work): One method for spotting fake transactions in a blockchain network has been the use of machine learning. Several supervised learning methods, including support vector machines, decision trees, logistic regression, and dense neural networks, were examined as part of this strategy. Accuracy examines every technique in-depth from a comparison perspective. This research may include a comparative analysis of unsupervised algorithms like as clustering. We also want to do in-depth future study on fraud on a private blockchain.

REFERENCE

[1] Joshi, P., Kumar, S., Kumar, D., & Singh, A. K. (2019, September). A blockchain based framework for fraud detection. In 2019 Conference on Next Generation Computing Applications (NextComp) (pp. 1-5). IEEE.

[2] Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. Financial Innovation, 2(1), 1-10.

[3] Dhiran, A., Kumar, D., & Arora, A. (2020, July). Video Fraud Detection using Blockchain. In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 102-107). IEEE.

[4] Nerurkar P, Bhirud S, Patel D, Ludinard R, Busnel Y, Kumari S. Supervised learning model for identifying illegal activities in Bitcoin. Appl Intell. 2020;209(1):1- 20.

[5] Ostapowicz, M., & Żbikowski, K. (2020, January). Detecting fraudulent accounts on blockchain: a supervised approach. In International Conference on Web Information Systems Engineering (pp. 18-31). Springer, Cham.

[6] Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K. Y. (2018, February). A blockchain framework for insurance processes. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-4). IEEE.

[7] Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A secure ai-driven architecture for automated insurance systems: Fraud detection and risk measurement. IEEE Access, 8, 58546-58558.

[8] Shanmuga Priya P and Swetha N, "Online Certificate Validation using Blockchain", Special Issue Published in Int. Jnl. Of Advanced Networking and Applications (IJANA).

[9] Monamo, P. M., Marivate, V., & Twala, B. (2016, December). A multifaceted approach to bitcoin fraud detection: Global and local outliers. In 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 188-194). IEEE.

[10] Xu, J. J. (2016). Are blockchains immune to all malicious attacks? Financial Innovation, 2(1), 1-9.

[11] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[12] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[13] K. Elissa, "Title of paper if known," unpublished.