International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Detection & Prevention of Credit card Fraud using Emerging Techniques of Block-chain & Machine Learning

Manish Rana, Rahul Khokale*[2], Sunny Sall[3] , Suresh R. Mestry[4] , Mahendra S. Makesar[5]

Submitted:11/03/2024 **Revised**: 26/04/2024 **Accepted**: 03/05/2024

Abstract:With the emergence of new digital India and the shift towards digital payments globally, fraudsters are finding ways to defraud financial institutions, resulting in loss of public money. Electronic payments have their own disadvantages. As the number of users increases, credit card fraud also increases at the same rate. Some people's credit card information may be collected without the owner's permission and used in fraudulent transactions. The problem of finding a credit card is to understand how many credit card frauds have occurred using historical credit data and create ML models. The resulting pattern is used to determine whether a new transaction is fraudulent. The model will then incorporate blockchain technology to ensure its success. Banking will be safer in the future. This will make fraud detection faster and more accurate.Credit card fraud costs thousands of dollars each year. Therefore, fraud detection is important for financial institutions to reduce their losses. The strategy presented in this article is an attempt to minimize financial losses. Additionally, the solution introduces the idea that the system will prevent fraud before it enters the blockchain.

Keywords: *Credit Card, Commercial Fraud, Machine Learning, Block chain.*

1. Introduction

Fraud can be defined as fraudulent or illegal acts committed for the purpose of obtaining money or personal wealth. This is a practice of increasing inequality. We get insights from valid or invalid payment information to make decisions . Many parameters include IP addresses, geographic location, historical transaction patterns, and patterns to identify such events. According to the World Payments Report, total noncash transactions increased by 10.1% from 482.6 billion in 2015 to 482.6 billion in 2016. Therefore, noncash transactions are expected to increase in the future. Fraud, which is dangerous for financial institutions, is also on the rise. During this global pandemic, most people are spending money without spendingmoney.Therefore, such a research platform needs to be established within a few years in order to reduce the losses of banks and financial institutions.

1.1. Machine Learning in Credit Card Fraud Detection

Machine learning provides machine "learning capabilities." Without explicit warning, machines can use previously received data and evaluate it in more detail. These features are useful for detecting credit card fraud. This makes it possible to successfully use machine learning algorithms in the banking industry to identify risky transactions. More than a million transactions occur every day, and each transaction must be verified to be valid. To achieve this goal, the system can be trained to distinguish fraud from non-fraud. This is usually done by giving it data from past transactions (especially data from fraudulent transactions) so that all future transactions can be classified as normal or suspicious. Those who are not suspicious will be separated for further examination.

1.2. Blockchain

A blockchain is a growing list of data, called blocks, that are cryptographically linked together. Each block contains the cryptographic hash of the previous block as well as the time.Variable data (usually represented as a Merkle tree). Blockchain is designed to prevent data transfer. It is an open, decentralized ledger that efficiently and permanently records transactions between parties.
Blacklist: Uses artificial intelligence and machine learning models to detect behavior or illegal elements in assets/data/transactions flowing into the blockchain, even inside or outside the blockchain.
White List: Banks have control over all credit cards they issue, when the credit card expires or is stolen, the bank can use technology to protect the value of the credit card through confirmation.

[1]*St. John College of Engineering & Management (SJCEM)Palghar-401404 , INDIA*
ORCID ID : 0000-0003-3765-9821
[2]*G H Raisoni University (GHRU)Saikheda, Maharashtra -480337 , INDIA*
ORCID ID : 0000-0001-7554-6903
[3] *St. John College of Engineering & Management (SJCEM)Palghar-401404 , INDIA*
ORCID ID : 0000-0002-8955-4952
[4]*Rajiv Gandhi Institute of Technology (RGIT), Andheri Mumbai-400061 , INDIA*
ORCID ID : 0009-0001-7579-3629
[5]*Nagpur Institute of Technology (NIT), Nagpur, Maharashtra -441501 , INDIA*
ORCID ID : 0000-0001-8960-6778
*** Corresponding Author Email:**manishrana23@gmail.com, dr.manish_rana@yahoo.com,softrahul2018@gmail.com,sunny_sall@yahoo.co.in,suresh.mestry@mctrgit.ac.in, mahendramakeshwar@gmail.com*

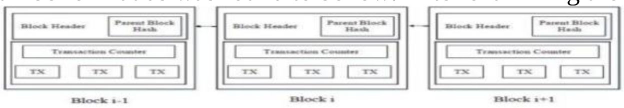


Fig 1: Structure of Blockchain. [5]

1.3. Valid information

A data set is a set of interrelated data. We use random data in this article.

Nonequivalent data have different values. This document contains information regarding transactions made with European cards. In two days, 284,807 transactions were recorded and 492 of them were determined to be fraudulent. The number of frauds was found to be low. After examining the main components of true quality, 28 characteristics were found. The time and price of the delivered products do not change and are in their original condition.

2. LITERATURE SURVEY

Table:1.1 Literature Survey

Paper Title	Author	Year of Publication	Idea/Methodology/ Concept	Features	Gap Identification
Credit Card Fraud Prevention Using Blockchain [5]	E.M.S.W Balagolla; W.P.C Fernando; R.M.N.S Rathnayake; M.J.M.R.P Wijesekera; A. N. Senarathne; K.Y. Abeywardhana	2021	This project includes a scaling mechanism to blockchain because the current projects have a lack of scalability. Furthermore, the solution incorporates proactive anomaly detection to detect fraudulent credit card transactions, with the system blocking frauds before they enter the blockchain.	Due to its intermediary parties, the proposed blockchain with fraud detection technology will help to prevent fraudulent credit card transactions. The authors suggest a solution (B-Box.com) in which credit card transactions are modelled on a blockchain, allowing for decentralized and verified credit card processing with an accredited set of computing nodes.	Paper was more inclined towards Smart Contracts based system as present in Ethereum blockchain but a generalized solution wasn't present.
Detecting Fraudulent Accounts on Blockchain: A Supervised Approach [9]	Michal Ostapowicz, Kamil Żbikowski	2019	We can use the idea presented in this paper to create a fraud detection flow for our project.	We use supervised learning approaches to detect fraudulent accounts on the Ethereum blockchain in this article. The paper had used 13 different explanatory variables used in Ethereum Blockchain and processed them via random forest, SVM, XGBoost algorithms.	The paper was based on accounts present on Blockchain Ledger and not in particular Fraud detection for Credit Card.
Credit Card Fraud Detection using Machine Learning and Data Science [3]	S P Maniraj, Aditya Saini, Swarna Deep Sarkar Shadab Ahmed	2019	Focused on analysing and pre-processing data sets as well as the deployment of multiple anomaly detection algorithms	On the PCA transformed Credit Card Transaction data, author used the Local Outlier Factor and Isolation Forest algorithm based on outlier's approaches and the work of Weng – Fu's research article.	Based on outliers' method and now more advanced methods are available
Fraud Detection in Credit Card Data using	Arun Kumar Rai, Rajendra	2020	Use of NN, along with unsupervised learning.	Compared Neural networks, auto encoders, local outlier	Used Neural Networks, which is bit complex and

Unsupervised Machine Learning Based Scheme [20]	Kumar Dwivedi			factor, isolation forest and kNN	might result into delay in detection.
Credit card fraud identification based on unbalanced data set on fusion model [21]	Donglin li	2019	The author has tried the algorithms lasso logistic algorithm & XGBoost algorithm. And then combined to form the fusion of both.	The fusion model has the highest prediction accuracy among both non defaulting and defaulting user, hence has a good extrapolation.	The model doesn't focus on over fitting and underfitting scenarios.
Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison [1]	Samidha Khatri Aishwarya Arora Arun Agrawal	2020	Various Machine learning supervised technique were applied on the dataset to tackle the problem of credit card fraud	Idea of Using Supervised and unsupervised learning together. Used Major Supervised learning algorithms and then proceeded with the one with highest accuracy.	The model was very basic and was focused in applying one algorithm at a time rather than combining two plus for better performance
Research on Credit Card Fraud Detection Model Based on Distance Sum [2]	Wen-Fang YU Na Wang	2009	The author has applied outlier algorithm to detect the credit card fraud	First step towards CC fraud detection using Models. Mathematically proved outliers. Had a strong base and was best of its time.	The technique which was used was too old and accuracy was also too low with 90% as compared to another algorithms
Machine Learning and Blockchain for Fraud Detection : Employing Artificial Intelligence in the Banking Sector[22]	Vinita Silaparasetty	2018	The Author has applied Blockchain technology with ML generated model	Tried to secure the Banking transactions with introduction of Block Chain	--------

The Literature Survey talks about various papers which having similar research .It shows the papers with title, Author Details, year of Publication, idea/Methodology/ Concept used by the authors , features extracted. From this literature survey various gaps were identified to forecast the problem definitions and highlight gaps on which methodology can be applied to remove gaps and improve results.

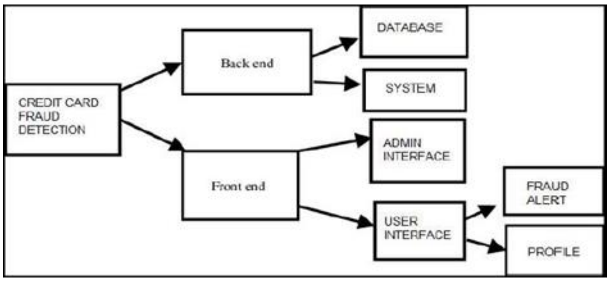


Fig 2: Module Diagram

3. Architectural Design

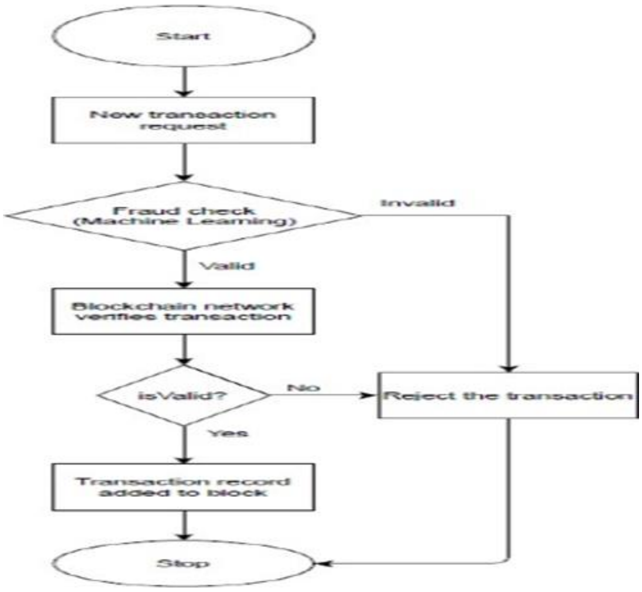

Start
New transaction request
Fraud check (Machine Learning)
Invalid
Valid
Blockchain network verifies transaction
isValid?
No
Reject the transaction
Yes
Transaction record added to block
Stop

Fig 3: Blockchain Block Contents

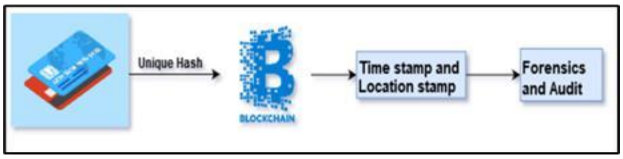


Fig 4: Fraud Detection Model in Action (1)

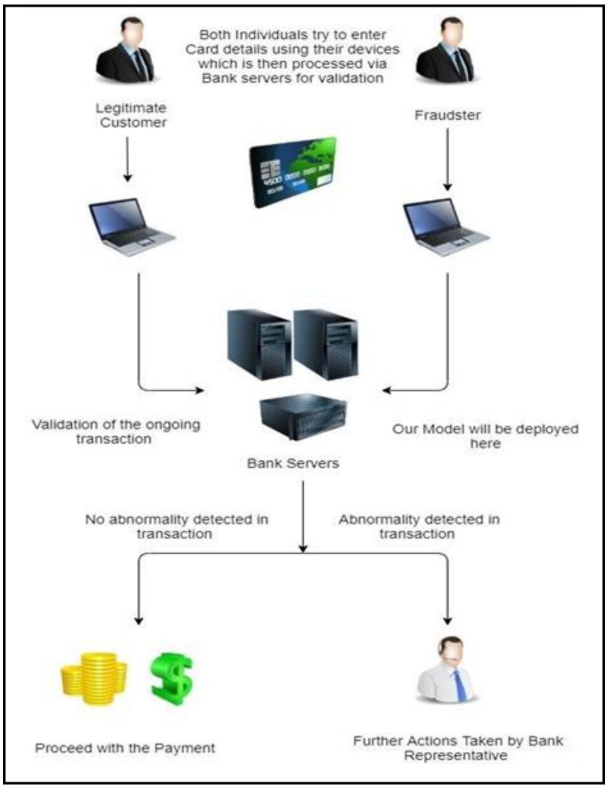

Both Individuals try to enter Card details using their devices which is then processed via Bank servers for validation
Legitimate Customer
Fraudster
Validation of the ongoing transaction
Bank Servers
Our Model will be deployed here
No abnormality detected in transaction
Abnormality detected in transaction
Proceed with the Payment
Further Actions Taken by Bank Representative

Fig 5: Fraud Detection Model in Action (2)

4. Research Method

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). This applies to papers in data storage**.** For example, write “15 Gb/cm^2 (100 Gb/in^2).” An exception is when English units are used as identifiers in trade, such as “3½-in disk drive.” Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

The SI unit for magnetic field strength H is A/m. However, if you wish to use units of T, either refer to magnetic flux density B or magnetic field strength symbolized as $\mu_0 H$. Use the center dot to separate compound units, e.g., “A·m^2.”

Surveying students and researching data before beginning to develop and propose a new credit card fraud module. Reviewed approximately 25+ pieces of information about advertising in newspapers and received 128 responses to the survey.

Detection of credit card fraud often relies on inconsistent information. Another idea is to convert unbalanced data into balanced data and then use the distribution model. It focuses solely on unsupervised learning followed by supervised data distribution. Group, categorize and segment data to find patterns and detect fraud.

Most current systems use outlier algorithms with 90% accuracy. When monitoring standards have been used recently.

1. The data set may have a lot of room for improvement. As mentioned before, the accuracy of the algorithm increases as the data set size increases.
2. However, this must be supported by the bank itself.
3. Fraud is a huge problem in the credit card industry and has become even more serious as electronic money transfers have become.
Popular. Therefore, the opportunity to improve the model will help the financial ecosystem.
4. The information is not balanced, meaning most transactions are not fraudulent, making it difficult to detect fraud.
5. Blockchain can reduce transaction times and create a secure ecosystem.

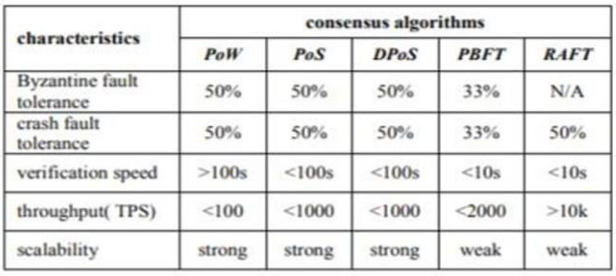
5. Benefits

Be aware of the different meanings of the homophones “affect” (usually a verb) and “effect” (usually a noun), “complement” and “compliment,” “discreet” and “discrete,” “principal” (e.g., “principal investigator”) and “principle” (e.g., “principle of measurement”). Do not confuse “imply” and “infer.”

Machine learning is a common choice for fraud. In this project, we tried to integrate with blockchain. For now, we use blockchain to store transaction information and time. Forensic institutions can use this special entry into the blockchain ledger for audits.

As it can be seen in Fig 5 “Fraud Detection Model in Action “which give a clear idea about the techniques been used to detect fraud through bank serves while proceeding with payment transaction.

Table I: Comparison between Consensus Methods [22]

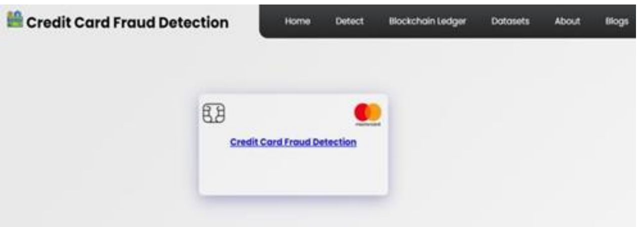


characteristics	consensus algorithms				
	PoW	*PoS*	*DPoS*	*PBFT*	*RAFT*
Byzantine fault tolerance	50%	50%	50%	33%	N/A
crash fault tolerance	50%	50%	50%	33%	50%
verification speed	>100s	<100s	<100s	<10s	<10s
throughput(TPS)	<100	<1000	<1000	<2000	>10k
scalability	strong	strong	strong	weak	weak

The table below clearly shows the characteristics of Byzantine fault tolerance, Crash fault tolerance, Verification speed, throughput (TPS) and Scalability. And compared in terms of Consensus algorithms (PoW, PoS, DpoS, PBFT, RAFT).

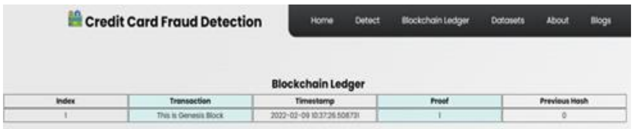
Guidelines for Graphics Preparation and Submission Proposed system is similar with Bitcoin technology for ledgers, Proof of Work is the best consensus method to choose.

6. Graphics Preparation and Submission Proposed



Credit Card Fraud Detection

Fig 6: Homepage

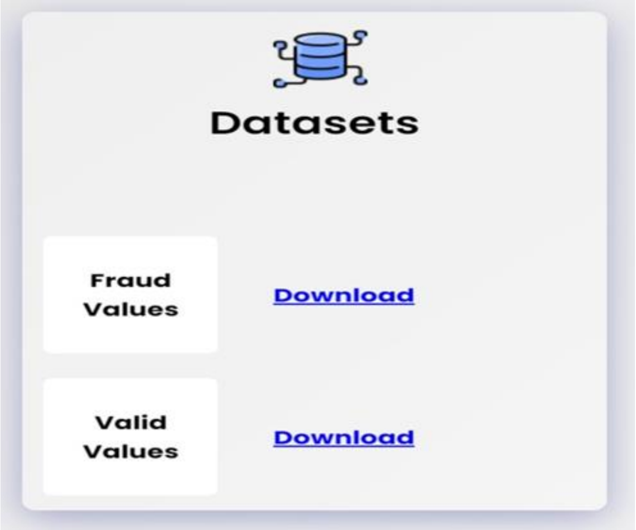


Credit Card Fraud Detection

Blockchain Ledger

Index	Transaction	Timestamp	Proof	Previous Hash
1	This is Genesis Block	2022-02-09 10:37:26.508731	1	0

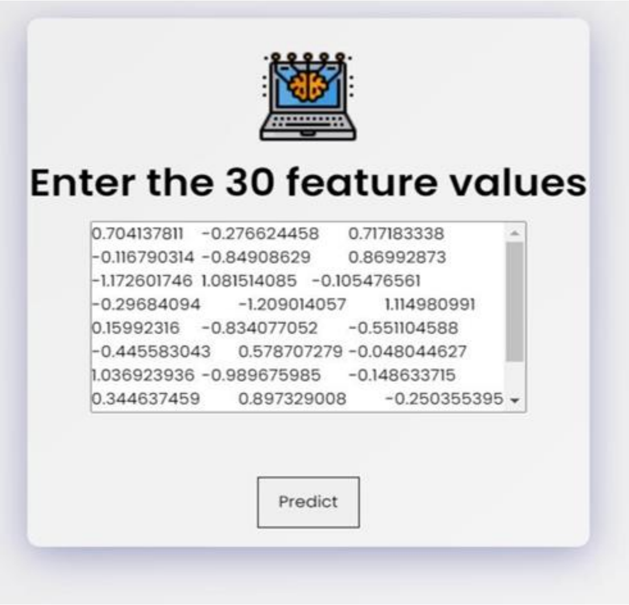
Fig 6a. Homepage of Credit Card fraud Detection



Datasets

Fraud Values	Download
Valid Values	Download

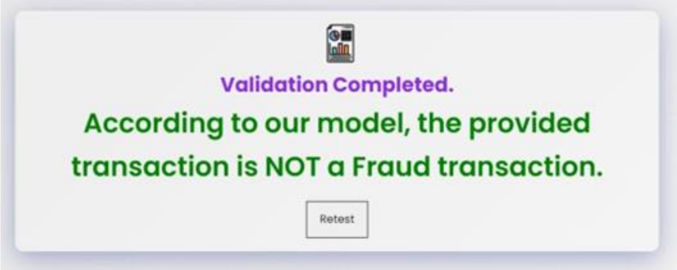
Fig 7: Sample Datasets



Enter the 30 feature values

```
0.704137811   -0.276624458    0.717183338
-0.116790314 -0.84908629      0.86992873
-1.172601746 1.081514085  -0.105476561
-0.29684094      -1.209014057       1.114980991
0.15992316    -0.834077052     -0.551104588
-0.445583043     0.578707279 -0.048044627
1.036923936 -0.989675985    -0.148633715
0.344637459        0.897329008        -0.250355395
```

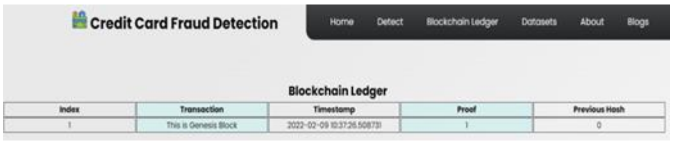
Fig 8: Input Cell



Validation Completed.

According to our model, the provided transaction is NOT a Fraud transaction.

Fig 9: Model Results

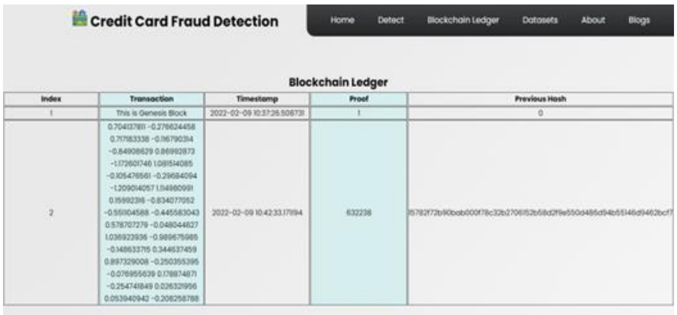


Credit Card Fraud Detection

Blockchain Ledger

Index	Transaction	Timestamp	Proof	Previous Hash
1	This is Genesis Block	2022-02-09 10:37:26.508731	1	0

Fig 10: Genesis Block



Credit Card Fraud Detection

Blockchain Ledger

Index	Transaction	Timestamp	Proof	Previous Hash
1	This is Genesis Block	2022-02-09 10:37:26.508731	1	0
2	0.704137811 -0.276624458 0.717183338 -0.116790314 -0.84908629 0.86992873 -1.172601746 1.081514085 -0.105476561 -0.29684094 -1.209014057 1.114980991 0.15992316 -0.834077052 -0.551104588 -0.445583043 0.578707279 -0.048044627 1.036923936 -0.989675985 -0.148633715 0.344637459 0.897329008 -0.250355395 -0.076955639 0.178874871 -0.254741849 0.026321956 0.053940942 -0.208258788	2022-02-09 10:42:33.171194	632238	5782f72b90bab000f78c32b2706f52b58d2f9e550d486d94b55146d9462bcf7

Fig 11: Addition of a Transaction to a block

7. Distribution and version control

We will use Heroku (https://www.heroku.com/), a platform as a service, to deliver our project. We use Flask (micro w eb application) to make the web application and Gunicorn as the web server interface.

We use GitHub for version control and push the fork from Heroku.

8. Conclusion

Decentralization, stability, security and immutability are some of the features of blockchain. With the advancement of technology, blockchain has become increasingly popular in many areas. Combining the power of blockchain with machine learning will help detect fraud. Theproject module is shown in Figure 2. The main components have been completed and tested. TheProject has completed its cloud deployment. The scope of the project can be expanded to research goals and research as a whole.

9. Future Scope

Scammers, phishers, hackers, and other organizations are always looking for opportunities to steal your credit card information. The accuracy of the model can be improved by adding more information; this can be done by working with banks.

Blockchain implementation and machine learning are challenging for us and we are currently in the early stages of the blockchain technology space.

Since Blockchain requires a lot of effort, new systems will be developed in the coming years and using blockchain at this scale will be both cost-effective and environmentally friendly.

The development of new recommendation algorithms may also affect the feasibility of the proposed strategy.

9.1. Appendix

Credit Card Fraud Detection Using Machine Learning and Blockchain DOI
Link: https://doi.org/10.22214/ijraset.2023.52214

9.2. Acknowledgment

This work carried out on “Detection & Prevention of Credit card Fraud using emerging techniques of Block-chain & Machine Learning” is a team afford, the team is acknowledged to put their best experimental result to show cast the outcome achieved and show in this paper.

10. References and Footnotes

10.1. References

References, referred in the preparation of manuscript, shows the highlight of the work carried by different researches worked in same domain, and provided, the platform to improve the results. And discuss the gaps which were show in literature survey.

Acknowledgements

This research was supported/partially supported by [1St. John College of Engineering & Management (SJCEM), Palghar-401404

, INDIA], G H Raisoni University (GHRU) Saikheda, Maharashtra -480337, INDIA, Rajiv Gandhi Institute of Technology (RGIT), Andheri Mumbai-400061, INDIA.

We thank our colleagues from [SJCEM] ,[GHRU] & [RGIT] who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. We thank [Dr. Rahul Khokale, Dr. Sunny Sall, Mr. Suresh R. Mestry &] for assistance with [particular technique, methodology], for comments that greatly improved the manuscript.

Author contributions

Manish Rana & Rahul Khokale : Conceptualization, Methodology, Software, Field study **Sunny Sall & Suresh R. Mestry:** Data curation, Writing-Original draft preparation, Software, Validation., Field study **Dr. Mahendra S.Makesar:** Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] S. Khatri, A. Arora, and A. P. Agrawal, "Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison," in *Proc. 2020 10th Int. Conf. on Cloud Computing, Data Science & Engineering (Confluence)*, 2020, pp. 680-683, doi: 10.1109/Confluence47617.2020.9057851.

[2] W. Yu and N. Wang, "Research on Credit Card Fraud Detection Model Based on Distance Sum," in *Proc. 2009 Int. Joint Conf. on Artificial Intelligence*, 2009, pp. 353-356, doi: 10.1109/JCAI.2009.146.

[3] S. P. Maniraj, A. Saini, S. Ahmed, and S. D. Sarkar, "Credit Card Fraud Detection using Machine Learning and Data Science," *Int. J. Eng. Res. & Technol. (IJERT)*, vol. 08, no. 09, pp. 1-6, Sep. 2019, doi: 10.17577/IJERTV8IS09003.

[4] S. Sorournejad, Z. Zojaji, R. E. Atani, and A. H. Monadjemi, "A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective," *arXiv*, [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1611/1611.06439.pdf.

[5] E. M. S. W. Balagolla, W. P. C. Fernando, R. M. N. S. Rathnayake, M. J. M. R. P. Wijesekera, A. N. Senarathne, and K. Y. Abeywardhana, "Credit Card Fraud Prevention Using Blockchain," in *Proc. 2021 6th Int. Conf. for Convergence in Technology (I2CT)*, 2021, pp. 1-8, doi: 10.1109/I2CT51068.2021.9418192.

[6] Y. Cai and D. Zhu, "Fraud detections for online businesses: a perspective from blockchain technology," *Financ. Innov.*, vol. 2, no. 20, 2016, doi: 10.1186/s40854-016-0039-4.

[7] M. Ostapowicz and K. Żbikowski, "Detecting Fraudulent Accounts on Blockchain: A Supervised Approach," in *Proc. Web Information Systems Engineering (WISE)*, 2019, pp. 1-12, doi: 10.1007/978-3-030-34223-4_2.

[8] S. Patil, V. Nemade, and P. Soni, "Predictive Modelling For Credit Card Fraud Detection Using Data Analytics," *Procedia Comput. Sci.*, vol. 132, pp. 385-395, 2018, doi: 10.1016/j.procs.2018.05.199. [9] V. Filippov, L. Mukhanov, and B. Shchukin, "Credit card fraud detection system," in *Proc. 2008 7th IEEE Int. Conf. on Cybernetic Intelligent Systems*, 2008, pp. 1-6, doi: 10.1109/UKRICIS.2008.4798919.

[9] K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions," in *Proc. 2017 Int. Conf. on Intelligent Computing and Control (I2C2)*, 2017, pp. 1-5, doi: 10.1109/I2C2.2017.8321781.

[10] K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions," in *Proc. 2017 Int. Conf. on Intelligent Computing and Control (I2C2)*, 2017, pp. 1-5, doi: 10.1109/I2C2.2017.8321781.

[11] J. O. Awoyemi, A. O. Adetunmbi, and S. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in *Proc. 2017 Int. Conf. on Computing Networking and Informatics (ICCNI)*, 2017, pp. 1-9, doi: 10.1109/ICCNI.2017.8123782.

[12] S. C. Dubey, K. S. Mundhe, and A. A. Kadam, "Credit Card Fraud Detection using Artificial Neural Network and BackPropagation," in *Proc. 2020 4th Int. Conf. on Intelligent Computing and Control Systems (ICICCS)*, 2020, pp. 268-273, doi: 10.1109/ICICCS48265.2020.9120957.

[13] K. R. Seeja and M. Zareapoor, "FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining," *The Scientific World Journal*, vol. 2014, Article ID 252797, 10 pages, 2014, doi: 10.1155/2014/252797.

[14] N. Malini and M. Pushpa, "Analysis on credit card fraud identification techniques based on KNN and outlier detection," in *Proc. 2017 Third Int. Conf. on Advances in Electrical Electronics, Information, Communication and Bio-Informatics (AEEICB)*, 2017, pp. 255-258, doi: 10.1109/AEEICB.2017.7972424.

[15] E. M. Carneiro, L. A. Vieira Dias, A. M. Da Cunha, and L. F. Stege Mialaret, "Cluster Analysis and Artificial Neural Networks: A Case Study in Credit Card Fraud Detection," in *Proc. 2015 12th Int. Conf. on Information Technology - New Generations*, 2015, pp. 122-126, doi: 10.1109/ITNG.2015.25.

[16] P. Kopyt et al., “Electric properties of graphene-based conductive layers from DC up to terahertz range,” *IEEE THz Sci. Technol.*, to be published, doi: 10.1109/TTHZ.2016.2544142.

[17] J. J. Xu, “Are blockchains immune to all malicious attacks?,” *Financ. Innov.*, vol. 2, no. 1, pp. 1-10, Dec. 2016, doi: 10.1186/s40854-016-0046-5.

[18] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. 2017 IEEE Int. Conf. on Systems, Man, and Cybernetics (SMC)*, 2017, pp. 2567-2572, doi: 10.1109/SMC.2017.81230.

[19] R. Rai and R. K. Dwivedi, "Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme," in *Proc. 2020 Int. Conf. on Electronics and Sustainable Communication Systems (ICESC)*, 2020, pp. 421-426, doi: 10.1109/ICESC48915.2020.9155615.

[20] Li, "Credit card fraud identification based on unbalanced data set based on fusion model," in *Proc. 2019 IEEE 1st Int. Conf. on Civil Aviation Safety and Information Technology (ICCASIT)*, 2019, pp. 235-239, doi: 10.1109/ICCASIT48058.2019.8973167.

[21] V. Silaparasetty, "Machine Learning and Blockchain for Fraud Detection: Employing Artificial Intelligence in the Banking Sector," in *Proc. 2018 GCU Int. Knowledge Transfer Conclave*, ISBN 978-93-86516-46-6, [Online]. Available: https://www.academia.edu/40207849/Machine_Learning_and_Blockchain_for_Fraud_Detection_Employing_Artificial_Intelligence.