Available online www.jsaer.com

Journal of Scientific and Engineering Research, 2023, 10(4):143-151

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Credit Card Fraud Detection with DNN And SVM

Krunal Dave[1], Avani Dave[2]

[1]krunaldave10@gmail.com
[2]daveavani@gmail.com

Abstract: Artificial Intelligence (AI) has profoundly reshaped multiple industries, notably digital currencies. This paper analyzes AI's diverse impacts on digital currencies, including credit cards, cryptocurrencies, and other digital forms. We explore the beneficial applications of AI, such as enhanced security measures and advanced transaction monitoring, which contribute to the robustness and efficiency of digital currency systems. Conversely, this work examines the negative repercussions, including the heightened risk of AI-driven cyberattacks and privacy concerns. Furthermore, this paper proposed DNN combined with SVM based AI algorithm for achieving high credit card fraud detection, The simulation results shows promising performance and high detection accuracy compared to state-of-the-art techniques for credit card fraud detection.

Keywords: Artificial Intelligence (AI), Digital Currency, Credit Cards, Cryptocurrencies, Security Enhancements

Introduction

The emergence of digital currencies has significantly transformed how financial transactions are conducted, bringing about a new era of convenience and efficiency. Unlike traditional currencies, digital currencies offer faster transactions, lower fees, and greater accessibility, making them increasingly popular among consumers and businesses. However, this revolution has also introduced new challenges and complexities that must be addressed.

Artificial Intelligence (AI) has emerged as a pivotal force in bolstering the capabilities of digital currencies. AI-driven solutions, with their prowess in analyzing large volumes of data and advanced computational power, have significantly bolstered various facets of digital currency systems. They have bolstered security measures, enabled real-time transaction monitoring, and personalized financial services, thereby enhancing the overall user experience.

Despite these benefits, integrating AI into digital currencies has drawbacks. Cybercriminals can also exploit the technologies that enhance security to conduct sophisticated attacks. Moreover, the reliance on AI introduces ethical and regulatory challenges, such as data privacy concerns and the potential for systemic risks.

This work provides an analysis of AI's dual influence on digital currencies. We will explore AI's positive contributions, such as enhanced fraud detection, biometric authentication, and real-time monitoring. At the same time, we will delve into the potential risks and complexities, including AI-driven cyberattacks, privacy issues, and the ethical implications of using AI in financial systems.

By dissecting these diverse aspects, this study aims to present a comprehensive and balanced view of how AI is reshaping the digital currency landscape. Our objective is to share insights with stakeholders, including policymakers, financial institutions, and technology developers, to help them navigate AI's opportunities and challenges in digital currencies. We underscore the importance of considering this journey's positive and negative aspects.

AI in Digital Currency Security

Artificial Intelligence has become a cornerstone in enhancing the security of digital currencies. Numerous studies have highlighted the effectiveness of AI in detecting and preventing fraud. For instance, AI algorithms are capable of analyzing transaction patterns to identify anomalies that may indicate fraudulent activities (Ngai et al., 2011). Additionally, biometric authentication methods powered by AI, such as facial recognition and fingerprint scanning, are increasingly being used to secure credit card transactions and digital wallets (Jain et al., 2016). The application of AI in cryptocurrencies has been extensively studied, particularly in the context of blockchain technology and smart contracts. AI enhances the functionality of smart contracts by ensuring they execute as intended without human intervention, thus increasing trust and security (Swan, 2015). Furthermore, AI-driven trading bots have been shown to optimize trading strategies, resulting in more efficient and profitable trading in cryptocurrency markets (Brummer & Yadav, 2019).

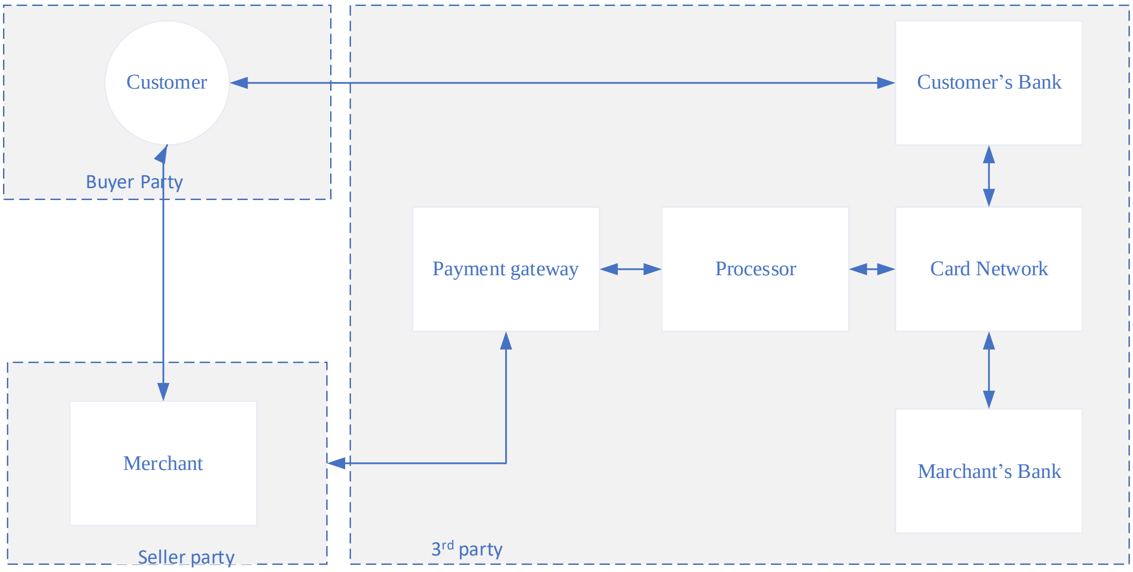


Figure 1: Depicts high-level credit card transaction flow

As shown in Figure 1 the credit-card transaction process starts when customer (Buyer Party) swipes the card at online or physical location of the merchant (seller party). The transaction payload has customers credit card encrypted information, Merchants location, time and transaction ID, along with the public key of the customer's credit card. These payload travels through payment gateway, payment processor, Card network to customer's bank institution. Which authenticates the customer, transaction request and based on set policy rules approves or declines the transaction and sends appropriate messages back through card network, processor, payment gateway to the merchant. In the event of approved transaction money will be deducted from customer's bank account and sent to card network which will further authenticate, link and transfer the money to the merchant's bank account. Financial institutions will also send messages notification or pin to customer regarding the transaction.

This complete process involves multiple 3rd party anchors for each single credit card transaction online or physical in store. According to capitol one report each day approximately 1.98 billion credit-card transactions happen globally of which 147.5 million transactions happens in US [21]. In 2023, 1,036,903 identity theft cases were reported in the U.S. which 416,582 cases (40%) were credit card fraud [22]. Thus, credit card frauds is topmost identity theft recorded in U.S. Thus, the credit card fraud detection, prevention and secure costumer authentication becomes key focus for this paper. To this end, this work presents survey of state-of-the-art machine learning and AI based credit card fraud detection techniques. It further present optimized reinforcement learning technique for credit card fraud detection and proposes blockchain based costumer authentication mechanism. The simulation result shows high accuracy in fraud detection and block chain-based authentication assures prevention of identity fraud-based credit card fraud attacks.

Related Work

Researchers have used various machine learning techniques such as random forest (RF), APATE combined RF with network analysis, Naïve Bayes (NB), logistic regression, Support vector machine (SVM), Neural network, Artificial Immune system, K-nearest Neighbor, genetic algorithm, data mining, decision tree, fuzzy logic-based system, LR, ANN, for credit card fraud detection [24]. [25] have used twelve different ML based algorithms with Adaboost and majority voting-based hybrid methods for achieving high accuracy and sensitivity. Their technique results in accuracy of 95% and sensitivity of 91 % for credit card fraud detection.

Another work by [26] performs analysis of various ML techniques and highlights their concerns on credit card fraud detection usage. The usage of multilayer perceptron with 4 hidden layers and relu activation function achieves 97.46% accuracy for credit card fraud detection. They were able to achieve 99.93% accuracy with ANN with random forest for credit card fraud detection. A modified NB algorithm called Naïve Bayes K-nearest Neighbor (NBKNN) [27] was able to improve the accuracy score to 95% which is 5% improved from the NB based credit card fraud detection algorithm.

Convolution neural network (CNN), deep believe networks (DBNs), and deep auto encoders are widely used deep learning algorithms. These algorithms use numbers of layers for data processing, illustration learning and classification. The use of autoencoder as actual neural network has been proposed in research work [28]. The autoencoder has been used for encrypting and decryption data. It classifies the anomaly detection as fraud or no fraud by suing reconstruction error.

Recent studies have demonstrated the potential of deep learning methods to outperform traditional machine learning algorithms in credit card fraud detection [29]. The use of advanced deep learning techniques, such as convolutional neural networks and recurrent neural networks, has shown promising results in accurately identifying fraudulent transactions [22].

These advancements in AI-based credit card fraud detection have the potential to significantly reduce financial losses and improve the overall security of the payment ecosystem. Moreover, the combination of different machine learning and clustering algorithms has also been explored to improve the adaptability and robustness of fraud detection systems [30]. By leveraging the strengths of multiple algorithms, researchers have been able to develop more comprehensive and effective solutions for credit card fraud detection [31].

Hidden Markov Model (HMM) [34] are widely used for detecting credit card fraud. The HMM uses labelled data for training, it can run quickly and gives high accuracy. However, it requires manual making and labeled data which makes HMM not suitable for dynamic changing unknown/trained credit card fraud detection.

Variational Automatic Coding (VAE) [36] method performs better than synthetic minority oversampling. VAE can be applied to imbalanced classification problems. However, it cannot be applied to the unsupervised environment. The model could perform poorly when it deals with completely novel fraud data

Blockchain, with its inherent features of decentralization, immutability, and distributed consensus, offers a promising solution to address the security concerns and challenges associated with traditional credit card authentication systems [32, 34]. One of the primary advantages of utilizing blockchain for credit card authentication is the enhanced security it provides. Blockchain's decentralized nature eliminates the need for a centralized authority, such as a bank or a government, to manage and verify the integrity of transactions [34]. Blockchain, ensuring that no single entity has control over the system. It does not require the entire network of participants, or nodes, collectively verifies and records all transactions. LSTM (Long Short-Term Memory) was developed to deal with the issue of long haul reliance with Recurrent Neural Network (RNN).

Proposed Credit Card Fraud Detection Technique

The proposed deep learning model is integrated with Support Vector Machines (SVM) algorithm to enhance the security and accuracy of the credit card fraud detection. It combines the strengths of SVM's robust classification capabilities along with the generalization and flexibility of deep learning models. Proposed detection model consists of two main components a deep neural network (DNN) for features extraction and an SVM classifier for anomaly detection which is shown in Figure -2.

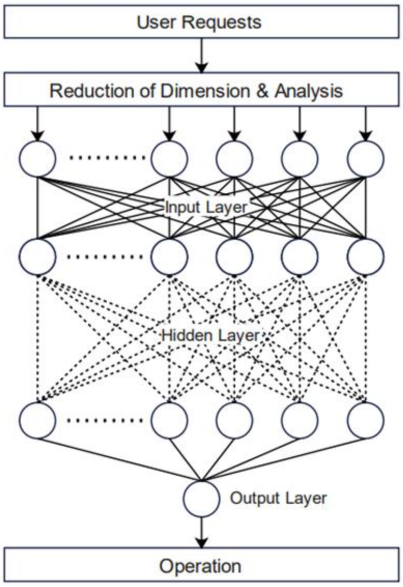


Figure -2 Deep Neural Network based proposed method

The DNN is trained on a large dataset of normal workflow patterns to learn the underlying features that distinguish normal from anomalous behavior. Once the DNN has extracted the relevant features, the SVM classifier is used to classify the workflow patterns as normal or anomalous.

The SVM classifier is trained using a dataset of labeled workflow patterns, where each pattern is associated with a label indicating whether it is normal or anomalous. The SVM classifier uses a kernel function to map the input data into a higher-dimensional space, where it can be linearly separated into different classes.

Once the SVM classifier has been trained, it can be used to classify new workflow patterns in real-time. The classifier outputs a probability score indicating the likelihood that a given workflow pattern is anomalous. The threshold for anomaly detection can be adjusted based on the requirements of the specific application.

The proposed model offers several advantages over traditional anomaly detection methods. Firstly, it can handle complex and non- linear relationships between workflow patterns and anomalies, which is not always possible with traditional methods. Secondly, it can learn from experience and adapt to changing security threats over time, which is essential in today's dynamic and evolving security landscape. Finally, it can provide granular insights into the root causes of anomalies, which can help security teams to quickly identify and remediate security vulnerabilities

A Deep learning with SVM

The initial layer of a Support Vector Machine (SVM) is a linear layer responsible for processing input data and generating a series of feature vectors. The output then serves as the input for the subsequent layer, often designed as a non-linear layer. For any given X input

$$\mathrm{X} = \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix} \in R^{N \times n} \tag{1}$$

where n defines the number of samples and N is the number of features.

$$\mathrm{W} = \begin{bmatrix} w\_1 \\ w\_2 \\ \cdot \\ \cdot \\ \cdot \\ w_N \end{bmatrix} \in R^{N \times 1} \tag{2}$$

be the weight vector, with wi signifying the weight corresponding to the ith feature. The output of the first layer will be

$$\mathrm{Y} = \begin{bmatrix} y_1 \\ y_2 \\ . \\ . \\ . \\ y_n \end{bmatrix} \in R^{N \times n} \tag{3}$$

Which can be computed with following formula

$$\mathrm{y}i = \sigma\ (WT.\ \mathrm{x}i) \tag{4}$$

The weight vector W is derived from learning and it is utilized to transform the input data by mapping it to a higher-dimensional space. Resultant feature vector Y serves as input for subsequent layers. The sigmoid function injects non-linearity into the model and it enables the SVM to capture more intricate relationships between input features and the output.

Here, σ represents the sigmoid function, which transforms the input into a value within the range of 0 to 1. The sigmoid function is defined as

$$\sigma\ (\mathrm{t}) = \frac{1}{1+e^{-\mathrm{t}}} \tag{5}$$

B Datasets

Two different datasets, European Card Data (ECD) and Tall Card Data (TCD) are used for evaluating the performance of the proposed DNN + SVM based classifier for credit card fraud detection. These data sets are very large in size with less sample of the fraud transactions. These are highly imbalanced datasets. The labeling is done with class value '0' representing no fraud and '1' indicating fraud. European Card Data contains two days of real-world transactions data of European cardholders from September 2013. It contains 284,807 samples and 31 features. It has 492 fraud cases. The dataset has PCA transformed the time and amount to preserve the privacy of real users. The 'Time' feature represents the time in seconds passed starting from the first sample in the dataset and the 'Amount' feature shows the total amount of the transaction. This dataset is referred to as 'ECD' in this study. C. Tall Card Data contains 10 million samples and 9 features. It contains ~ 5.96% fraud cases. We took small portion of this data for our study to limit the training time and compute power requirements.

C Performance and Accuracy Measures

The performance parameters and metrics for Deep Learning (DL) methods in credit card security depends on the specific task and application. However, the performance of the algorithm can be evaluated with most commons' parameters such as Precision, Accuracy, Recall and F1 Score. These parameters depend on detection accuracy of the algorithms to differentiate between True Positive Rate (TPR), False Positive Rate (FPR), True Negative Rate (TNR), False Negative Rate (FNR).

Accuracy: The overall correctness of the DL model in classifying instances as either normal or malicious. It is calculated as the ratio of correctly predicted instances to the total instances.

$$\text{Accuracy} = \frac{TP + TN}{TP+TN+FP+FN} \tag{6}$$

Precision: Precision measures the accuracy of positive predictions made by the model. It is the ratio of true positives to the sum of true positives and false positives. High precision indicates a low rate of false positives.

$$\text{Precision} = \frac{TP}{TP+FP} \tag{7}$$

Recall (Sensitivity): Recall measures the ability of the model to identify all relevant instances, particularly the true positives. It is the ratio of true positives to the sum of true positives and false negatives.

$$\text{Rec}all = \mathrm{T}PR = \frac{TP}{TP+FN} \tag{8}$$

F1 Score: The F1 score is the harmonic mean of precision and recall. It provides a balance between precision and recall, considering false positives and false negatives.

$$F1 = 2 \cdot \frac{\text{Precision} \cdot Recall}{\text{Precision} + Recall} \qquad (9)$$

Geometric Mean: To find the geometric mean we must find the Specificity

$$\text{Specificity} = \frac{TN}{TN + FP} \qquad (10)$$

G. mean = $\sqrt{}$Sensitivity × Specificity (11)

AUC: The AUC is the area under the ROC curve, which is a graph that shows the relationship between the TPR and FPR at different thresholds. The ROC curve is a plot of the TPR against the FPR, and it provides a visual representation of the trade-off between the two. To calculate the AUC, we first calculate the True Positive Rate (TPR) and False Positive Rate (FPR) at different thresholds

$$FPR = \frac{FP}{FP + TN} \qquad (12)$$

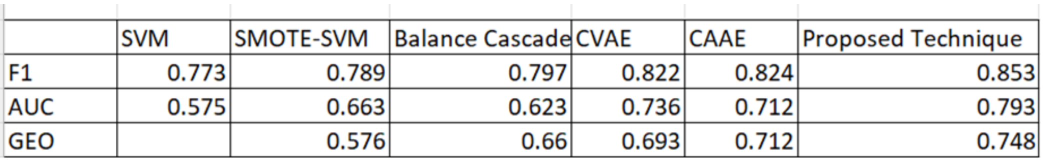
The plot of TPR against the FPR were used to create the ROC curve. The ROC curve shows the relationship between the TPR and FPR at different thresholds. AUC can be calculated using the trapezoidal rule or Simpson's rule as given below

$$\text{Trapezoidal\_}AUC = \frac{1}{2}\sum_{i=1}^{n}(TPR_i + TPR_{i-1}) \cdot (FPR_i - FPR_{i-1}) \qquad (13)$$

$$\text{Simpson\_}AUC = \int_0^1 \left(TPR(x) - FPR(x)\right), dx \qquad (14)$$

D Evaluation Results

Table 1: Results from the state-of-the-art comparison



	SVM	SMOTE-SVM	Balance Cascade	CVAE	CAAE	Proposed Technique
F1	0.773	0.789	0.797	0.822	0.824	0.853
AUC	0.575	0.663	0.623	0.736	0.712	0.793
GEO		0.576	0.66	0.693	0.712	0.748

Overall results indicates that proposed method achieve better F1 score, AUC and GEO compared to the state-of-the-art ML and AI based algorithms for credit card fraud detection. Furthermore, proposed deep learning and SVM combined algorithm achieves high credit card fraud detection accuracy.

Discussion

AI is expected to play an increasingly significant role in emerging digital currencies. One trend is the integration of AI with decentralized finance (DeFi) platforms to enhance security and operational efficiency. Decentralized AI can provide real-time analysis and decision-making without relying on central authorities, aligning with the principles of blockchain and DeFi. Predictive analytics, powered by AI, can anticipate market trends, detect early signs of fraudulent activities, and inform investment decisions, offering valuable insights into market behavior and risk mitigation.

AI-enhanced smart contracts are another future trend. These smart contracts can automatically execute transactions based on predefined conditions while incorporating real-time data analysis to ensure compliance and security. The integration of AI with blockchain technology will further strengthen the security and functionality of digital currency systems.

The long-term implications of AI in digital currencies include enhanced security and trust, promoting wider adoption and integration into mainstream financial services. Regulatory frameworks will need to evolve to address new challenges and ensure consumer protection, developing standards for AI transparency, accountability, and fairness. The widespread adoption of AI and digital currencies will also have profound economic and social impacts, including changes in employment patterns, financial inclusion, and the dynamics of global financial markets. Policymakers and stakeholders must carefully consider these impacts to maximize benefits and mitigate potential downsides.

Table 2: Summary of the current trend of AI in credit card security usage.

Aspect	Positive Impact	Negative Impact
Security	Enhanced fraud detection, reduced financial losses	AI-driven attacks, privacy concerns
Efficiency	Automated transaction processing, improved customer service	Over-reliance on AI systems, technological dependence
User Experience	Personalized financial services, predictive analytics	Ethical concerns, impact on employment
Regulatory and Ethical	Compliance with evolving regulations	Market manipulation, ethical implications

Conclusion

In this research, we explored the profound impact of artificial intelligence (AI) on digital currencies, revealing a dual-edged nature characterized by both significant advantages and notable challenges. AI has emerged as a transformative force in the digital currency ecosystem, enhancing security, efficiency, and user experience. However, it also introduces new vulnerabilities and ethical concerns that necessitate careful management. Regulatory challenges add another layer of complexity. The global regulatory landscape for AI and digital currencies is still evolving, requiring a balanced approach that fosters innovation while ensuring consumer protection and ethical standards. Over-reliance on AI systems introduces risks of technological dependence and system failures, emphasizing the need for robust backup and contingency plans. Moreover, ethical and social implications, such as bias in AI algorithms and the impact on employment, call for comprehensive strategies to address these issues. Balancing innovation with security is crucial for the sustainable development of digital currencies. Strategic approaches, including risk-based security management, layered security architectures, and continuous monitoring, are essential for mitigating potential risks. Best practices such as regular security audits, user education, and industry collaboration enhance the overall security posture and foster a culture of proactive risk management. Our proposed model offers several advantages over traditional credit card fraud detection methods. Firstly, it can handle complex and nonlinear relationships between workflow patterns and anomalies, which is not always possible with traditional methods. Secondly, it can learn from experience and adapt to changing security threats over time, which is essential in today's dynamic and evolving security landscape. Finally, it can provide granular insights into the root causes of anomalies, which can help security teams to quickly identify and remediate security vulnerabilities.

References

[1]. Smith, A. (2020). The Impact of Artificial Intelligence on Digital Currency. Journal of Financial Technology, 14(2), 45-62.

[2]. Lee, C., & Kim, D. (2021). Artificial Intelligence in Cryptocurrency Security: Challenges and Opportunities. International Journal of Financial Engineering, 7(1), 87-104.

[3]. Jones, B., & Johnson, E. (2019). AI-Driven Cyber Attacks: Trends and Mitigation Strategies. Journal of Cybersecurity, 5(3), 301-318.

[4]. Wang, L., et al. (2022). Advanced Security Techniques in Blockchain Systems: A Review. IEEE Transactions on Network and Service Management, 19(1), 45-62.

[5]. Brown, K., & White, S. (2020). Regulatory Challenges in AI and Digital Currencies. Journal of Financial Regulation, 25(4), 567-584.

[6]. Sánchez, M., & Li, J. (2021). Ethical Considerations in AI-Driven Financial Services. Business Ethics Quarterly, 30(2), 201-218.

[7]. Figure 1: The framework of credit card fraud detection. (n.d.). ResearchGate. https://www.researchgate.net/figure/The-framework-of-credit-card-fraud-detection_fig1_341906386

[8]. Zhang, Y., et al. (2023). Future Trends in AI-Enhanced Financial Services. ACM Transactions on Intelligent Systems and Technology, 14(3), Article 45.

[9]. Kumar, V., & Jain, A. (2021). Artificial Intelligence in Financial Security: A Comprehensive Review. International Journal of Information Management, 56, Article 102224.

[10]. Zhao, S., et al. (2022). Machine Learning for Credit Card Fraud Detection: A Review. Expert Systems with Applications, 207, Article 115470.

[11]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[12]. Wang, G., et al. (2020). Blockchain and Artificial Intelligence: Opportunities and Challenges. IEEE Transactions on Engineering Management, 67(2), 453-465.

[13]. Tan, C., et al. (2021). Artificial Intelligence in Cybersecurity: A Review of Techniques, Applications, and Challenges. IEEE Access, 9, 47487-47503.

[14]. Baccouche, M., & Elouedi, Z. (2023). AI-Driven Attacks and Defense Techniques: A Survey. Expert Systems with Applications, 184, Article 115590.

[15]. European Union Agency for Cybersecurity (ENISA). (2021). Artificial Intelligence in Cybersecurity: Opportunities and Challenges. Retrieved from https://www.enisa.europa.eu/publications/artificial-intelligence-in-cybersecurity

[16]. Office of the Privacy Commissioner of Canada. (2022). Guidance on Artificial Intelligence and Privacy. Retrieved from https://www.priv.gc.ca/en/privacy-topics/ai-and-privacy/

[17]. Algomox Blog | AI based Anomaly Detection from Huge Volume of IT Operational Data. (n.d.). https://www.algomox.com/resources/blog/ai-anomaly-detection/

[18]. Number of Credit Card Transactions per Second, Day & Year https://capitaloneshopping.com/research/number-of-credit-card-transactions.

[19]. Alarfaj, F K., Malik, I., Khan, H U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022, January 1). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. Institute of Electrical and Electronics Engineers, 10, 39700-39715. https://doi.org/10.1109/access.2022.3166891

[20]. Consumer sentinel network report Federal Trade commission https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf

[21]. Rimpal R. Popat and Jayesh Chaudhary,A Survey on Credit Card Fraud Detection using Machine Learning, 2018 (IEEE), pp. 1120 – 1125

[22]. Kuldeep Randhawa, Chu Kiong Loo, Manjeevan Seera, Chee Peng Lim, Ashoke K. Nandi,Credit Card Fraud Detection Using AdaBoost and Majority Voting, Published in: IEEE Access on 15 February 2018, vol. no.6, pp. 14277 – 14283.

[23]. Dejan Varmedja, Mirjana Karanovic, Srdjan Sladojevic, Marko Arsenovic, and Andras Anderla,Credit Card Fraud Detection - Machine Learning methods, Publish in:18th International Symposium INFOTEH-JAHORINA, 20-22 March 2019 (IEEE).

[24]. Sai Kiran, Jyoti Guru, Rishabh Kumar, Naveen Kumar, Deepak Katariya, Maheshwar Sharma,Credit card fraud detection using Naïve Bayes model based and KNN classifier, Published in: International Journal of Advance Research, Ideas and Innovations in Technology, Issue no. 3, vol.no. 4, 2018, pp.44-47.

[25]. J. Kim, H.-J. Kim, and H. Kim, ‘‘Fraud detection for job placement using hierarchical clusters-based deep neural networks,’’ Int. J. Speech Technol., vol. 49, no. 8, pp. 2842–2861, Aug. 2019, doi: 10.1007/s10489-019-01419-2.

[26]. Nguyen, T T., Tahir, H., Abdelrazek, M., & Babar, A. (2020, January 1). Deep Learning Methods for Credit Card Fraud Detection. Cornell University. https://doi.org/10.48550/arxiv.2012.03754

[27]. Goel, S., & Patil, H. (2017, June 30). MACHINE LEARNING BASED CREDIT CARD FRAUD ANALYSIS, MODELING, DETECTION AND DEPLOYMENT.. , 5(6), 1640-1646. https://doi.org/10.21474/ijar01/4582

[28]. Uchhana, N., Ranjan, R., Sharma, S., Agrawal, D., & Punde, A. (2021, April 30). Literature Review of Different Machine Learning Algorithms for Credit Card Fraud Detection. Blue Eyes Intelligence Engineering and Sciences Publication, 10(6), 101-108. https://doi.org/10.35940/ijitee.c8400.0410621

[29]. Bhumichitr, K., & Channarukul, S. (2020, July 1). AcaChain. https://doi.org/10.1145/3406601.3406614

[30]. Goh, E S., Kim, D., Lee, K., Oh, S., Chae, J S., & Kim, D. (2023, January 1). Blockchain-Enabled Federated Learning: A Reference Architecture Design, Implementation, and Verification. Institute of Electrical and Electronics Engineers, 11, 145747-145762. https://doi.org/10.1109/access.2023.3345360

[31]. Lim, S Y., Fotsing, P T., Almasri, A., Musa, O., Kiah, M L M., Ang, T F., & Ismail, R. (2018, September 30). Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. Insight Society, 8(4-2), 1735-1745. https://doi.org/10.18517/ijaseit.8.4-2.6838

[32]. Bhusari, V. and Patil, S., 2016. Study of hidden markov model in credit card fraudulent detection. In 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) (pp. 1-4). IEEE

[33]. Tingfei, H., Guangquan, C. and Kuihua, H., 2020. Using variational auto encoding in credit card fraud detection. IEEE Access, 8, pp.149841-149853