International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Fraud Prediction and Verification of Smart Credit Card Using Machine Learning Techniques

Dr.B.U.Anu Barathi[1], Baswaraj Prajapnoor[2], Praveen Kumar[3]

[1]Assistant Professor, Sathyabama institute of Science and Technology, Chennai – 600127, India
[2]Computer Science and Engineering, Sathyabama institute of Science and Technology, Chennai – 600127, India

ABSTRACT
This study unveils a powerful method for smart credit card fraud detection and verification. This system integrates data preprocessing, feature engineering, and real-time prediction using a hybrid model that incorporates supervised machine learning algorithms, an encoder, and LSTM networks. A supervised LSTM network sorts transactions, while an unsupervised Autoencoder finds outliers. Assessment criteria strike a balance between recall and accuracy. Alerts are sent by the system upon detection of fraud, and it runs in real-time. Compliance, scalability, and constant monitoring are key points. To close the gap between ease and safety in contemporary monetary transactions, this project offers a state-of-the-art method for strengthening the security of smart credit cards.

Keywords: LSTM, AUTOENCODER, ANOMALY

I. INTRODUCTION

With the introduction of smart credit cards, a new age of frictionless and speedy monetary transactions has begun. The use of these highly developed payment systems has simplified the day-to-day financial transactions for both consumers and enterprises. But with the proliferation of smart credit cards comes a new and ever-present danger: credit card theft.The ever-evolving methods used by criminals to take advantage of loopholes in the system make combating credit card theft an enormous problem. Successfully countering this threat requires the development of novel and flexible solutions. This study addresses this urgent requirement by introducing a thorough method is smart credit card fraud prediction and verification using hybrid machine learning. An extensive dataset including a variety of smart credit card transactions is first collected and preprocessed as part of the project's multi-faceted approach. The dataset contains both valid and fraudulent transactions, making it a valuable resource for building models.

An unsupervised Autoencoder neural network is a key component of this study because of how well it detects outliers in transaction data. Using the encoder component of the Autoencoder to learn latent characteristics, this method can identify fraud even when it's not immediately obvious. Supervised machine learning methods, including LSTM networks—well-suited to sequence data—are used in the research to improve prediction accuracy. To improve the model's capacity to differentiate between real and fraudulent transactions, the LSTM network is taught using the encoded characteristics obtained by the

Autoencoder.To guarantee that this hybrid model can withstand the rigors of real-world use, it is tested extensively utilizing a wide range of performanlllce indicators. Finding the sweet spot between detecting a large number of fraudulent transactions and avoiding false positives requires optimizing recall and precision criteria. Implementation in real time is one of the main objectives of the project. The technology is built to handle credit card transactions in real-time, responding instantly to any signs of possible fraud. To reduce losses and safeguard cardholders, alerts may be set up and predetermined actions can be executed.

The project's concept is based on the idea of continuous monitoring and modification. The ever-changing nature of fraud tendencies is recognized, highlighting the need of continuously improving models and updating data. To further guarantee the system's ethical and legal operation, compliance with data privacy laws and regulatory frameworks is an essential factor to consider.A major step forward in smart credit card security is essentially what this initiative is all about. In an ever-more-digital and linked world, it aims to secure cardholders and financial institutions by combining state-of-the-art machine learning methods with real-time capabilities, striking a careful balance between the two.

II. RELATED WORKS

1. The study by Saraswathi, P., Kulkarni, E., Khalil, M. L., and Nigam, S. D. (2019) recommends an artificial neural network and self organizing maps for the prediction and detection of credit card fraud. The 2019 Third International Conference on Computing Methodologies and Communication features a presentation of their research. The study's objective is to create a sophisticated credit card verification system that can quickly detect and stop fraudulent transactions. The authors emphasize the opportunity to improve the precision and effectiveness of credit card fraud detection by merging artificial neural networks and self-organizing maps.
2. The approach for preventing credit card fraud that Chowdary, Kundan, and Mary (2019) propose makes use of multiple authentications. Improved smart credit card verification is the system's goal. The authors explain their work in the IOP Conference Series: Engineering, and Material Science emphasizing the value a strong and trustworthy authentication method in combating credit card fraud. Their work supports current initiatives to create safe smart credit card systems.
3. To improve smart credit card verification, Sadgali et al. (2020) offer an adaptive approach on credit card fraud detection. The goal of the project to create in intelligent system that can quickly and accurately identify fraudulent transactions. The model may adapt and change over time to effectively identify new and developing fraud tendencies thanks to the use of machine learning algorithms. According to the experts, this adaptive strategy has a lot of potential for enhancing the security and dependability of credit card verification systems.
4. Logistic regression and k fold machine learning techniques were used in a study on fraud prediction on smart societies by Mishra and Pandey (2021). Their study concentrated on using these methods for smart credit card verification. The objective of the study was to improve credit card transaction security through accurate fraud prediction and prevention. The study's conclusions offer important guidance for creating reliable fraud detection systems in advanced nations.
5. A Bidirectional Gated Recurrent Unit (Bi-GRU) model is suggested by Sadgali, Sael, and Benabbou (2021) in order to improve credit card fraud detection. By incorporating the Bi-GRU architecture into the credit card verification process, the study seeks to increase classification accuracy. The

performance of the suggested model is assessed using a dataset of credit card transaction records. The outcomes demonstrate the Bi-GRU model's potential for use in smart credit card verification systems by showing how well it performs in comparison to current techniques.

6. In the context of 5G networks, Unal, Hammoudeh, and Kiraz (2020) examine the policy specification and verification aspects of smart contracts and blockchain technology. Their research focuses on how these technologies can be used for smart credit card verification. The authors offer insights into the possible advantages and difficulties of deploying blockchain and smart contracts for secure credit card transactions in the 5G future by reviewing the literature and current practices. By their analysis, Unal et al. suggest a methodology for enhancing the dependability and integrity of credit card verification processes in 5G networks by incorporating policy formulation and verification approaches.
7. A blockchain based safe multipurpose identity management system for smart cities is suggested by Rahat et al. (2022). The system attempts to make credit card verification procedures more secure and effective. The system makes sure that user identities are securely controlled by utilizing blockchain technology, which reduces instances of fraud and unauthorized access. Smart credit card verification systems in smart cities could become much more dependable and trustworthy thanks to the suggested method.
8. Code cloning in smart contracts, particularly in the context of verified contracts from the Ethereum blockchain platform, is the main topic of Kondo et al. (2020)'s study. To examine the frequency and effects in code cloning on these contract, they undertake a case study. In their article, the authors seek to shed light on the security flaws that code cloning could introduce in smart credit card verification systems. Their empirical investigation highlights the necessity for programmers to handle code cloning difficulties in order to improve the security and dependability of smart contract-based credit card verification procedures.
9. A machine learning-based Cibil verification system was created by Rani, G. S., Reddy, A. T., Vardhan, V. B., Harsha, A. S. B., and Sakthimohan, M. in 2020 for smart credit card verification. The article offers details on the design and operation of this system, which was presented at the 2020 Third International Conference on Smart System and Inventive Technologies.
10. In their study, Duela et al. (2023) suggest a decentralized payment architecture for utilities and ecommerce transactions that incorporates government verified IDs. By utilizing this architecture, their study focuses on improving smart credit card verification, opening the door for more safe and effective online transactions.

III. EXISTING SYSTEM

There are a number of drawbacks to the current smart credit card verification method that reduce its effectiveness and efficiency. The existing system, for starters, mainly relies on magnetic stripe technology, which is prone to data theft and cloning. The cardholders are at a high risk of fraud and illegal transactions since the information contained on the magnetic stripe is readily available and copyable**.** The current credit card fraud prediction system in banking support relies on basic rule-based methods and simple anomaly detection techniques. This approach lacks the ability to effectively capture complex patterns in fraudulent activities, leading to high false positives and negatives.

The current system also frequently has compatibility and interoperability problems. Rule-based systems utilize predefined criteria, making them rigid and prone to false positives and negatives. Meanwhile, traditional machine learning models may not effectively capture temporal dependencies and complex

patterns in transaction data. Due to the disparate standards that various nations and regions have established for credit card verification, there is a lack of standardization in the authentication procedures. This inconsistency presents substantial hurdles for international tourists and business owners as it may be challenging for them to use their smart credit cards in various locations, which could cause trouble and user annoyance.

Finally, both the user experience and transaction speed of the current system are constrained. When card terminals or networks are busy, the authentication process may occasionally take a long time. Longer transaction times and unsatisfied customers may result from this. Additionally, the transition to a seamless and effective digital payment environment is hampered by the reliance on physical cards and human data entry during distributions.

In conclusion, there are a number of drawbacks to the current smart credit card verification system, such as limited adaptability and accuracy result in delayed or inaccurate fraud detection, leading to financial losses for both financial institutions and cardholders. There is a pressing need for a more robust and proactive approach to combat the ever-evolving landscape of credit card fraud.

IV. PROPOSED SYSTEM

To detect and prevent smart credit card fraud, this study introduces a hybrid approach that integrates supervised machine learning, Autoencoder, and Long Short Term Memory (LSTM) networks. Prior to unsupervised anomaly detection using an Autoencoder, data is preprocessed and features are engineered. The next step in using encoded data for transaction classification is training a supervised LSTM network. LSTM, with its ability to model temporal dependencies, enhances the system's predictive capabilities. With real-time deployment, fraud may be detected immediately and notifications can be triggered if needed. Important characteristics include scalability, regulatory compliance, and continuous monitoring and modification. It results in precision, recall, F1-score and detection accuracy and integrates advanced feature engineering and ensembling to improve accuracy, robustness, false-positive rate, Integration with decision making systems and adapt to evolving fraud patterns, resulting in more precise fraud detection. Securing customers and financial institutions against the ever-changing danger of credit card fraud, this suggested system offers a strong solution that combines security with simplicity.

V. SYSTEM ARCHITECTURE

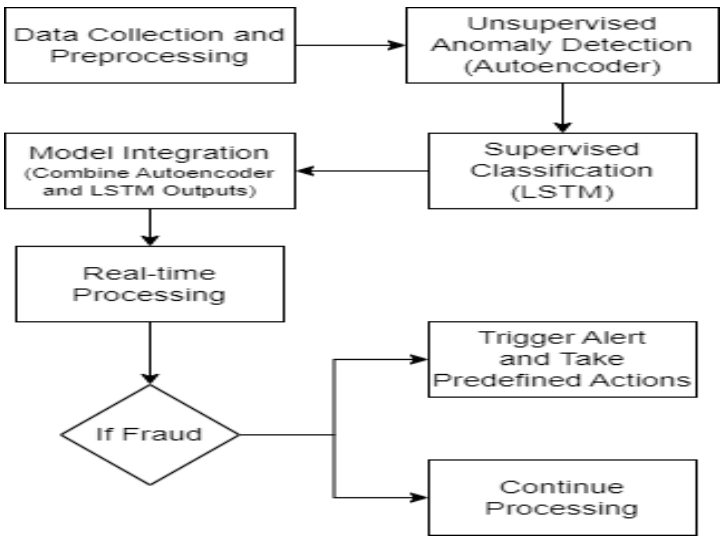

Fig. 1. System Architecture

VI. METHODOLOGY

1. Data Collection Module:

The Data Collection Module serves the foundation of system by sourcing smart credit card transaction data from diverse channels, encompassing real-time streams and historical records. It establishes the critical initial dataset, which forms the basis for the subsequent data-driven operations. This module interfaces with various data providers and APIs to retrieve transaction data efficiently, ensuring a continuous influx of information for fraud analysis.

2. Data Preprocessing Module:

The Data Preprocessing Module plays a pivotal role in refining the raw transaction data into a usable format. It conducts rigorous data cleaning, removing outliers, handling missing values, and rectifying inconsistencies. This module also conducts data transformation tasks like encoding categorical variables and normalizing numerical features, rendering the dataset compatible with machine learning algorithms. Its output serves as the foundation for feature engineering and model training.

3. Feature Engineering Module:

The Feature Engineering Module introduces sophistication to the raw transaction data by extracting informative attributes that contribute to the predictive power of the model. It discerns patterns within the data, creating novel features such as transaction amounts, merchant categories, and timestamps. These engineered features amplify the model's ability to distinguish legitimate transactions from fraudulent ones, facilitating more accurate predictions.

4. Unsupervised Anomaly Detection Module (Autoencoder):

The Unsupervised Anomaly Detection Module leverages the potent capabilities of deep learning through the Autoencoder neural network. This module's primary objective is to identify anomalies within the transaction data. It achieves this by training the Autoencoder to encapsulate the underlying structure of legitimate transactions. Any deviations or discrepancies between the original transaction data and their reconstructions by the Autoencoder are flagged as potential anomalies. This unsupervised approach is adept at detecting subtle, previously unseen fraud patterns.

5. Supervised Classification Module (LSTM):

The Supervised Classification Module harnesses the strengths of LSTM neural networks to provide supervised learning and classification. Utilizing the encoded features from the previous Autoencoder module and additional transaction attributes, this module categorizes transactions into two classes: legitimate or fraudulent. Through training on labeled data, the LSTM model learns to differentiate between transaction types, achieving a high level of accuracy in classification tasks.

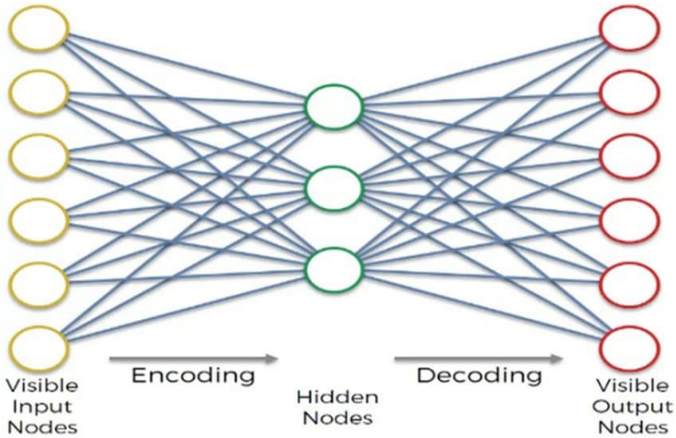

Fig.2: Autoencoder

6. Model Integration Module:

The Model Integration Module harmoniously merges the outputs of the Autoencoder and LSTM models. It potentially concatenates the encoded features from the Autoencoder with the classification results from the LSTM, creating a unified output that capitalizes on the strengths of both models. By integrating information from these two distinct sources, the module aspires to enhance the overall fraud prediction and verification capabilities.

7. Real time Processing Module:

The Real time Processing Module represents the operational heart of the system. It continually monitors incoming credit card transactions in real-time, ensuring prompt analysis and response. This module leverages the hybrid model developed in the previous steps to predict and verify the legitimacy of transactions. In cases where fraudulent transactions are detected, it triggers alerts and executes predefined actions to mitigate losses and secure cardholders.

VII. RESULT AND DISCUSSION

A highly developed and trustworthy way for ensuring the security and legality of credit card transactions is the smart credit card verification system. To safeguard cardholder information and stop fraud, this system employs a combination of technology and data encryption approaches. The smart card verification system examines a number of things when a credit card is used for a transaction, it gets the integrated information from both autoencoder and LSTM. If it discovers the possibility of a fraudulent transaction, it initiates alerts and carries out predetermined measures actions to diminish losses and safeguard cardholders.

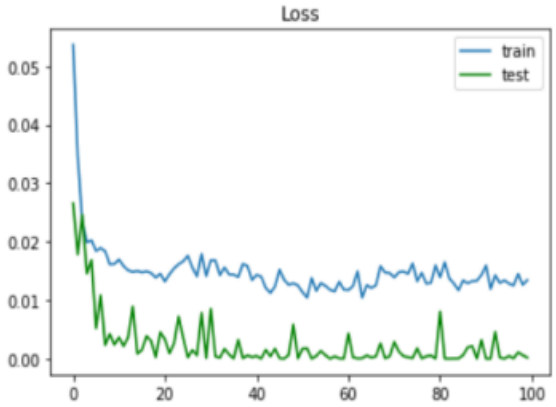

Fig 3: LSTM Loss Function

These many steps of verification give an extra layer of security and lower the possibility of fraud or identity theft. Additionally, the system continuously scans transaction data and patterns for anomalies or suspicious activity, immediately notifying both the cardholder and the institution issuing the card of any such activity. The system has the ability to stop payments in the case of fraudulent transactions and to open an investigation. This approach guarantees that transactions are safe and reliable while also safeguarding the cardholder's financial information and giving them piece of mind. Electronic payments are now much safer and more convenient thanks to the smart credit card verification system, which has become a crucial part of contemporary financial operations.

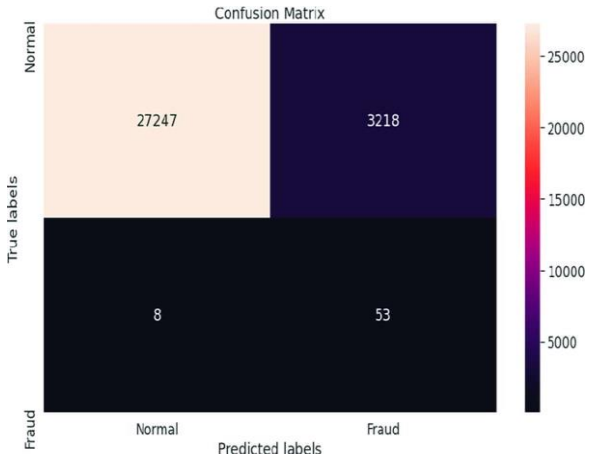

Fig.4. confusion matrix

TABLE 1: Results from Last 10 Epochs

Epoch	AUC	MSE	MAE
1	0.9953	0.0037	0.0067
2	0.9949	0.0042	0.0078
3	0.9956	0.0034	0.0063
4	0.9951	0.0039	0.0069
5	0.9955	0.0036	0.0066
6	0.9951	0.0038	0.0069
7	0.9953	0.0037	0.0067
8	0.9954	0.0036	0.0065
9	0.9951	0.0038	0.0069
10	0.9955	0.0035	0.0065

The Table 1 provides the metrics (AUC, MSE, MAE) for each epoch during model training.

VIII. CONCLUSION

In conclusion, the smart credit card verification system is a cutting-edge and effective way to guarantee quick and secure transactions. To increase security and stop fraud, it makes use of cutting-edge approach like fusion of Autoencoder and LSTM. This technology is built to handle credit card transactions in real-time, responding instantly to any signs of possible fraud. To reduce losses to further protect sensitive data, the use of hybrid technology showed promising results in precision, recall, F1-score and detection accuracy. This ensures that the real credit card information is not saved or shared during the transaction process. Overall, this clever credit card verification method gives users a practical and safe way to conduct transactions, lowering the possibility of fraud and providing security.

IX. FUTURE WORK

Further work on the smart credit card verification system will involve a number of crucial components that could improve its usability and security. it could explore advancements in machine learning and deep learning algorithms.This might involve experimenting with newer architectures, investigating ensemble

methods, or integrating cutting-edge techniques for improved predictive accuracy Secondly, by regularly examining patterns and behaviors related to credit card transactions, powerful artificial intelligence and machine learning algorithms can assist increase the accuracy of fraud detection. This can help in real-time fraud prevention and the detection of questionable activity. Exploring blockchain technology can also do away with the need for centralized databases, lowering the danger of data breaches and boosting privacy. Credit card information is stored and verified using blockchain technology. However, adopting a proactive security strategy, such as routinely doing penetration tests and vulnerability assessments, can assist in identifying and resolving any potential system problems. The smart credit card verification system may be adopted more widely and boost customer convenience and trust by providing smooth connection with different payment platforms and systems.

REFERENCES

1. Saraswathi, E., Kulkarni, P., Khalil, M. N., & Nigam, S. C. (2019, March). Credit card fraud prediction and detection using artificial neural network and self-organizing maps. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1124-1128). IEEE.
2. Chowdary, M. A., Kundan, M., & Mary, A. V. A. (2019, October). Effective credit card forgery prevention using multilevel authentication. In IOP Conference Series: Materials Science and Engineering (Vol. 590, No. 1, p. 012021). IOP Publishing.
3. Sadgali, I., Sael, N., & Benabbou, F. (2020). Adaptive model for credit card fraud detection.
4. Mishra, K. N., & Pandey, S. C. (2021). Fraud prediction in smart societies using logistic regression and k-fold machine learning techniques. Wireless Personal Communications, 119, 1341-1367.
5. Sadgali, I., Sael, N., & Benabbou, F. (2021). Bidirectional gated recurrent unit for improving classification in credit card fraud detection. Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 21(3), 1704-1712.
6. Unal, D., Hammoudeh, M., & Kiraz, M. S. (2020). Policy specification and verification for blockchain and smart contracts in 5G networks. ICT Express, 6(1), 43-47.
7. Rahat, A. H., Rumon, M. R., Joti, T. J., Tasnin, H., Akter, T., Shakil, A., & Hossain, M. I. (2022, January). Blockchain based secured multipurpose identity (SMID) management system for smart cities. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0737-0744). IEEE.
8. Kondo, M., Oliva, G. A., Jiang, Z. M., Hassan, A. E., & Mizuno, O. (2020). Code cloning in smart contracts: a case study on verified contracts from the Ethereum blockchain platform. Empirical Software Engineering, 25, 4617-4675.
9. Rani, G. E., Reddy, A. T. V., Vardhan, V. K., Harsha, A. S. S., & Sakthimohan, M. (2020, August). Machine Learning based Cibil Verification System. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 780-782). IEEE.
10. Duela, J. S., Raja, K., Umapathy, P., Rangnani, R., & Patel, A. (2023). Decentralized Payment Architecture for E-Commerce and Utility Transactions with Government Verified Identities. Soft Computing and Signal Processing: Proceedings of 5th ICSCSP 2022, 313, 9.
11. Forough J, Momtazi S. Ensemble of deep sequential models for credit card fraud detection; 2020. Tehran: Computer Engineering Department, Amirkabir University of Technology. Google Scholar
12. Jeragh M. Combining auto encoders and one class support vectors machine for fraudulant credit card transactions detection; 2018. Kuwait: Computer Engineering Department, Kuwait University, Mousa

AlSulaimi, Information Technology Department, Boubyan Bank. Google Scholar
13. Awoyemi JO, Adetunmbi AO, Oluwadare SA. Credit card fraud detection using machine learning techniques: a comparative analysis; 2017. Akure: Department of Computer Science Federal University of Technology Akure.Google Scholar
14. Zhang XHana YXua WWang QHOBA: a novel feature engineering methodology for credit card fraud detection with a deep learning architecture2019New YorkElsevierGoogle Scholar
15. Jiang P, Zhang J, Zou J. Credit card fraud detection using autoencoder neural network; 2019. Department of Electrical & Computer Engineer, University of Western Ontario.Google Scholar