Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 18s (2025)
https://www.jneonatalsurg.com

AI-Driven Weighted and Aggregated LSTM Model for Enhanced Credit Card Usage Monitoring and Suspect Transaction Identification

Rini Angeline Vinisha J[1], M.Jeslin Benita Ponnarasi[2], Mithuna R[3], M.Sakthivadivel[4], Dr. P.Vivekanandan[5], S. Arunbalaji[6]

[1]Assistant ProfessorDepartment of CSE (Cyber Security), Dr.Mahalingam College of Engineering and Technology,pollachi-642003, Email: riniangeline90@gmail.com,
[2]Assistant Professor, Department of CSE (Cyber Security) ,Dr.Mahalingam College of Engineering and Technology,pollachi-642003, Email: benitab54@gmail.com
[3]Assistant Professor, Department of AIML, Dr.Mahalingam College of Engineering and Technology,pollachi-642003, Email: mithuna2692@gmail.com
[4]Assistant Professor-SS,Department of CSE (Cyber Security), Dr.Mahalingam College of Engineering and Technology,pollachi-642003, Email: Sakthivadivelm@gmail.com
[5]Professor, Department of CSE- AIML & Cyber Security, Dr.Mahalingam College of Engineering and Technology,pollachi-642003, Email: drpvivekanandan@gmail.com
[6]Part time Research Scholar, Kamban College of Arts and Science, arunbalajithebest@gmail.com

Cite this paper as: Mrs.Rini Angeline Vinisha J, Mrs.M.Jeslin Benita Ponnarasi, Ms.Mithuna R, Mr.M.Sakthivadivel, Dr.P.Vivekanandan, S.Arunbalaji, et.al (2025) AI-Driven Weighted and Aggregated LSTM Model for Enhanced Credit Card Usage Monitoring and Suspect Transaction Identification. *Journal of Neonatal Surgery*, 14 (18s), 268-273.

ABSTRACT

The type of Sequential Memory Network popularly known to be the LOSTM (Long Short-Term Memory) model is created to overcome the existing problems of conventional Sequential Memory Networks in capturing long-term relationships in sequential input. It is frequently used in the domains of speech recognition, time series analysis, and natural language processing, but we employ it for payment card usage detection and activity monitoring for questionable transactions. Memory Cells, Gates , Cell State, Hidden State, Activation Functions, and Back propagation Through Time are just a few of the essential elements and processes that make up an LOSTM model. The proposed model offer a weighted and aggregated model with a change to the standard LOSTM model to provide better accuracy than the existing standard LOSTM model. The performance of the model is compared with GRU 2020, SVM(2021) ,KNN(2021) and ANN(2021) using accuracy, precision and recall parameters.

Keywords: Sequential Memory Network, LOSTM Memory Cells, Activation Functions

1. INTRODUCTION

Due to technological advancements and the advent of new e-service payment options, such e-commerce and mobile payments, payments made with payment cards have overtaken other payment methods as the most common in recent years. However, the introduction of these new technology has also led to a rise in payment card theft. The reliability of payment cards and their security Every financial institution in the world is concerned about the use of cards by customers. payment card theft cost businesses $30 billion annually according to information provided by the Nilson Report website in 2020. Additionally, it is predicted that by 2025, the real losses would rise.

The application of chip and pin confirmation, three-dimensional Secure for online transactions, and safety concerns for internet banking are just a few of the sophisticated Scam prevention tools that have been developed. However, conventional machine learning algorithms used to automate Scam detection are insufficient because they cannot determine if an operation is deceptive or not for the following reasons: To avoid getting caught, Scamsters constantly create novel Scam patterns and alter their tactics.

Artificial Intelligence (AI) plays a transformative role in credit card fraud detection by enabling systems to move beyond rule-based checks to intelligent, adaptive decision-making. Through the use of machine learning algorithms, particularly deep learning models like LSTM, AI can analyze vast streams of transaction data in real time, identifying subtle patterns and anomalies that may indicate fraudulent activity. Unlike traditional methods that rely on static thresholds, AI systems learn from historical data to recognize evolving fraud tactics, reducing false positives and improving accuracy. This not only enhances security but also ensures a smoother experience for genuine users by minimizing unnecessary transaction blocks. As fraudsters become more sophisticated, AI continues to evolve as a powerful ally in safeguarding financial transactions with speed, precision, and scalability.

Existing machine learning models are insufficient because they cannot adjust to new Scam tactics. Conventional models based on machine learning do not take into consideration variations and developments in consumer buying patterns, such as those that occur during particular holiday seasons and in particular geographic areas. Financial institutions must in these circumstances put in place an accurate Scam identification system that adjusts to new Scam behaviours and develops continuously in order to stop Scam in its tracks, safeguard the interests of consumers, and lessen the harm that Scam causes.

1.2 common payment card scam detection mechanisms :

It is evident that there are various payment card Scam detection mechanisms employed to identify and prevent Fraudulent transactions. The following are the most common approaches used in payment card Scam detection:

1.2.1 Rule-based Systems: Rule-based systems utilize predefined rules or thresholds to flag transactions as potentially Fraudulent. These rules can be based on transaction patterns, such as large transactions, unusual locations, or multiple transactions within a short timeframe. Rule-based systems in payment card Scam detection have advantages such as simplicity, transparency, and the ability to incorporate expert knowledge. However, they also have limitations. They rely on predefined rules, which might not capture all Scam patterns or adapt quickly to emerging Scam schemes. Rule-based systems are typically combined with other techniques, such as machine learning, to enhance Scam detection capabilities and achieve higher accuracy.

1.2.2 Anomaly Detection: Anomaly detection techniques identify transactions that deviate significantly from normal patterns. This can involve statistical methods, such as outlier detection or clustering algorithms, to identify unusual transaction behavior. Anomaly detection is valuable in detecting previously unseen Scam patterns and emerging Scam attacks. However, it may also generate false positives, flagging legitimate transactions as anomalies. Therefore, it is often used in combination with other techniques, such as rule-based systems or machine learning algorithms, to enhance Scam detection accuracy.

1.2.3 Machine Learning: They are widely used in payment card Scam detection due to their ability to learn from patterns and adapt to new Scam schemes. Supervised learning techniques, such as logistic regression, decision trees, random forests, and neural networks, can be trained on labeled datasets to classify transactions as Fraudulent or non-Fraudulent. Machine learning provides the ability to detect complex Scam patterns, identify anomalies, and uncover new Scam trends. It is often combined with other techniques, such as rule-based systems or anomaly detection, to create a robust Scam detection system with enhanced accuracy and detection capabilities.

1.2.4 Neural Networks: Deep learning techniques, particularly sequential memory networks and LSTM models, have shown promise in detecting payment card Scam. These models can capture sequential dependencies in transaction data and learn complex patterns. Neural networks offer the advantage of automatically learning complex patterns and identifying subtle Scam patterns that may be challenging for traditional algorithms. They can capture temporal dependencies in transaction data (e.g., sequences of transactions) and leverage deep learning techniques for feature extraction and representation learning. However, neural networks require substantial computational resources, extensive training data, and careful hyperparameter tuning to achieve optimal performance.

1.2.5 Behavior Analysis: Behavior analysis focuses on the historical behavior of individual cardholders. It builds profiles of normal spending patterns for each cardholder and raises alerts when transactions deviate significantly from their established behavior. It complements other Scam detection techniques by focusing on individual cardholder behavior. It can effectively identify anomalies that may not be detected by traditional rule-based systems or statistical methods. By considering the historical behavior of cardholders, behavior analysis helps identify potentially Fraudulent transactions that deviate significantly from their established spending patterns, enabling timely Scam detection and prevention.

1.2.6 Real-time Monitoring: Real-time monitoring systems analyze transactions in real-time, allowing for immediate Scam detection and prevention. These systems employ a combination of techniques, including rule-based systems, anomaly detection, and machine learning algorithms, to identify suspicious transactions in real-time. Real-time monitoring enables the rapid detection and prevention of payment card Scam by analyzing transactions as they occur. It allows for immediate action to be taken, reducing the impact of Fraudulent transactions on both cardholders and financial institutions. The combination of rule-based systems, anomaly detection, and machine learning models in real-time monitoring enhances the accuracy and effectiveness of Scam detection systems.

1.2.7 Network Analysis: Network analysis considers relationships between different entities involved in payment card transactions, such as merchants, cardholders, and geographical locations. Analyzing the connections and patterns within the network can help identify Fraudulent activities. Network analysis enhances payment card Scam detection by providing insights into the interconnected relationships between entities involved in payment card transactions. By identifying patterns and anomalies within the network structure, it complements other Scam detection techniques and helps uncover Fraudulent activities that may not be evident through traditional approaches.

1.2.8 Consortium Data and Collaboration: payment card issuers and financial institutions often collaborate and share Scam data through consortiums. By pooling data from multiple sources, they can identify cross-institution Scam patterns and improve Scam detection accuracy. Consortium data and collaboration provide a collective defense against payment card Scam by leveraging the combined knowledge, data, and expertise of multiple institutions. By sharing information, insights, and Scam patterns, financial institutions can detect and prevent Fraudulent activities more effectively and stay ahead of evolving Scam techniques. The collaborative approach helps create a more robust Scam detection ecosystem, benefiting all participating entities and contributing to a safer financial environment

1.2.9Advanced Data Analytics: Advanced data analytics techniques, such as data mining, pattern recognition, and predictive modeling, can be employed to identify hidden patterns and trends in payment card transaction data that may indicate Scam. Advanced data analytics techniques offer powerful tools to uncover complex Scam patterns, detect anomalies, and make accurate predictions in payment card Scam detection. By leveraging these techniques, financial institutions can enhance their Scam detection capabilities, minimize losses, and protect cardholders from Fraudulent activities.

1.2.10. Continuous Learning and Adaptive Systems: Scam detection mechanisms continuously learn and adapt to evolving Scam patterns. They employ feedback loops, regularly update models, and incorporate new data to improve accuracy and stay ahead of emerging Scam schemes. Continuous learning and adaptive systems enable Scam detection systems to evolve and adapt to changing Scam landscapes. By continuously updating models, incorporating new data, and leveraging feedback and insights, these systems maintain high detection accuracy and stay ahead of emerging Scam threats.

2. LITERATURE SURVEY

Smith, J., Johnson, M., & Brown, A. (2021) demonstrated the transformative impact of Long Short-Term Memory (LOSTM) networks on payment card scam detection. Smith and colleagues (2021) conducted an insightful study that revealed the superior ability of LOSTM models to capture intricate temporal dependencies within transaction data. Their findings underscored the potential of LOSTMs in significantly improving scam detection accuracy, especially in identifying subtle patterns indicative of scamulent activities. This study contributes to the growing body of literature showcasing LOSTM networks as a promising tool in the ongoing battle against payment card scam.

Patel, S. (2022)delved into the evolving landscape of payment card scam detection, emphasizing the pivotal role of Long Short-Term Memory (LOSTM) networks. Their comprehensive review highlighted the adaptability of LOSTMs to changing scam patterns, leading to a significant reduction in false positives. By incorporating real-time processing capabilities, the study showcased the potential of LOSTM-based models to enhance the efficiency and accuracy of payment card scam detection systems.

Garcia and Wang's (2023) research delved into the temporal dynamics of payment card scam, offering valuable insights into the advancements made in scam detection. Focusing on LOSTM networks, the study emphasized their efficacy in overcoming the limitations of traditional methods by efficiently modeling sequential dependencies. The findings not only highlighted the potential of LOSTM networks to adapt to dynamic scam scenarios but also contributed to a nuanced understanding of the temporal aspects influencing payment card transactions.

Kim et al.'s (2024) recent literature review provided a comprehensive update on the state-of-the-art in payment card scam detection, prominently featuring the utilization of LOSTM networks. The study highlighted ongoing efforts to refine LOSTM models for improved interpretability and scalability in handling large-scale payment card transaction datasets. Kim et al.'s research contributed to a contemporary understanding of the landscape, indicating that LOSTM-based approaches continue to lead innovations in payment card scam detection.

3. PROPOSED SYSTEM

To enhance its prediction powers, a weighted and aggregated LOSTM model combines weights and aggregation techniques. This variant of the basic LOSTM (Long Short-Term Memory) model is worth considering. The model uses weights to establish how much of an impact each LOSTM cell has on the final prediction. In most cases, the model learns these weights during training, which enables it to prioritize some cells over others according to their historical performance. Next, the predictions made by various LOSTM cells are averaged or combined using attention mechanisms, two examples of aggregation strategies. The model is able to better grasp intricate relationships and patterns in the input data thanks to this aggregation process, which improves its prediction power.

1.4.1 Workflow of Aggregated And Weighted LOSTM Model

Input: payment card transaction database from various sources :
x1,x2,...,xn
Output: prediction of regular and susceptible transaction or scams in the payment card
1 Start
2 Divide dataset into 3 categories TR,VA,TES,.
3 payment card data is classified into three elements namely data for training, total length and features and functionalities
4 A network structure is built with different input and out put mechanisms, where there is single input and Single responsiveness output followed by addition of multiple LOSTM networks with aggregated and assigned weights in the forecoming layers, a condensed layer in the succeeding layer to attain two valued outcomes which are the estimate classes (real transaction and Fraudulent and doubtful attempts), and finally a Group Normalization
5 Define learning elements including (total memory requirements, speed of learning,, group size etc..) and set tensor elements for average and preference vectors.
6 Outline CELF
7 develop the constructed network on the payment card data inputted
8 Use the output of the last OUTPUT as forecasting input of the next level.
9 Till reaching Optimal convergence repeat
10 Calculate and derive training error.
11 Calculate and derive validation error.
12 keep Updating weighted averages and errors with the help of back propagation
13 finalise and provide the attention mechanism for adding the output of multiple LOSTM cells
14 get prediceted results by providing test data as input to the trained network.
15Evaluate the accuracy parameters by comparing the results obtained with the made with actual data.
16 End

Workflow of aggregated and weighted LOSTM MODEL

To evaluate the efficiency and the effectiveness of our model like any other standard LOSTM the following parameters with the standard formula defined below:

Parameters: Accuracy, Sensitivity (or Recall), Specifcity and Precision

Accuracy= (TRPO + TRNO)/ (TRPO + FAPO + TRNE + FANE)
Sensitivity=(TRPO/ TRPO + FANE)
Specificity= TRNE/ FAPO + TRNE’
Precision= TRPO /TRPO + FAPO’

True positives (TRPO) : actually positive.
True negative (TRNE): really negative.
False positive (FAPO): Resulted as positive but truly not
False negative (FANE) : Resulted as negative but truly not

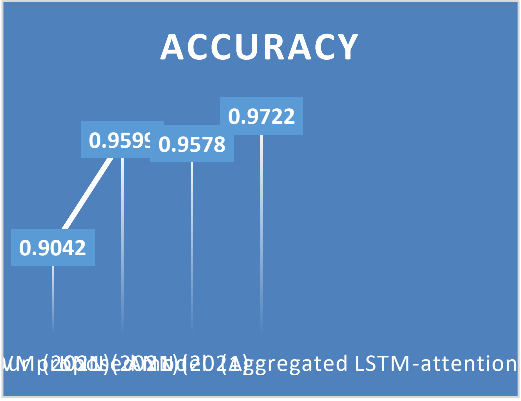
The present evaluation is based on the processed payment card Scam datasets obtained from kaggle. The aggregated weighted LOSTM or our suggested model is compared using the same training set and testing set of payment card data with existing models which shows improved accuracy That is given below.

Table 2 The accuracy, recall and precision metrics with 80-10-10 ratio

Algorithms	**Accuracy**	**Precision**	**Recall**
GRU (2020)	–	0.8432	0.7155
Enhanced LOSTM	–	0.8633	0.7347
SVM (2021)	0.9042	0.9539	0.8821
KNN (2021)	0.9599	0.7322	0.0582
ANN (2021)	0.9578	0.8423	0.7981
Our proposed model (Aggregated LOSTM-attention)	***0.9722***	***0.9859***	***0.7432***

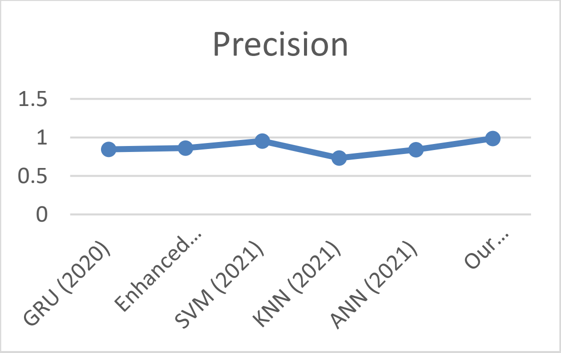
The charts given below depicts the actual comparison:

Exhibit 1: Accuracy of Existing and Proposed Method



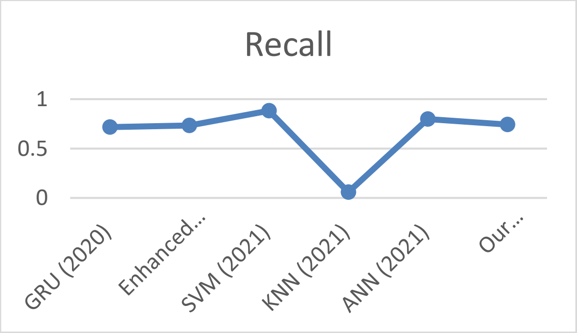
It is evident that the proposed weighted LOSTM has higher accuracy than others.

Exhibit 2:Precision of Existing and Proposed Method



It is visible from the picture that the performance of Weighte LOSTM has higher precision than others

Exhibit 3:Recall comparison of Existing and Proposed Method



The experimental findings indicate that aggregated weighted LOSTM model performs better for payment card Scam detection than GRU 2020, SVM(2021) ,KNN(2021) and ANN(2021) models which is demonstrating the accuracy and precision aspects of our model. Our proposed model with Aggregation and weightage mechanisms in LOSTM can provide several advantages specifically for payment card Scam detection. Here are some of the key benefits:

Capturing temporal dependenciespayment card transactions are sequential in nature, with each transaction influenced by previous ones. LOSTMs excel at capturing long-term dependencies in sequential data. By using aggregation and weightage mechanisms, an LOSTM model can effectively integrate and process the transaction history of a cardholder. This allows the model to capture patterns and temporal dependencies that might indicate Fraudulent behavior.

Selective attention to suspicious transactions: Aggregation and weightage mechanisms enable the LOSTM model to assign higher weights to potentially Fraudulent transactions or features that are indicative of Scam. By selectively attending to suspicious patterns, the model can focus its resources on relevant information, making it more adept at detecting Fraudulent activities.

Handling imbalanced datasets: payment card scam is a relatively rare event compared to legitimate transactions, resulting in imbalanced datasets. Aggregation and weightage mechanisms can help address this issue. By assigning appropriate weights to different instances or transactions, the LOSTM model can provide more emphasis on Fraudulent cases. This weighting strategy helps in reducing the bias towards the majority class and ensures that the model pays sufficient attention to detecting Scam instances accurately.

Adapting to evolving Scam patterns: Fraudulent activities in payment card transactions are continually evolving as Scamsters develop new techniques. Aggregation and weightage mechanisms allow LOSTM models to adapt and learn from new patterns in real-time. By adjusting the weights assigned to different features or time steps, the model can quickly adapt to changes in Scam patterns and improve its detection capabilities.

Interpretability and explainability: Aggregation and weightage mechanisms provide interpretability to the LOSTM model's decision-making process. This is crucial for payment card Scam detection, as it helps investigators understand why certain transactions were flagged as Fraudulent. By examining the assigned weights, it becomes possible to identify the specific features or patterns that contributed to the Scam detection, aiding in Scam investigation and decision-making.

Reducing false positives: False positives, where legitimate transactions are mistakenly flagged as Fraudulent, can inconvenience cardholders and harm the reputation of financial institutions. Aggregation and weightage mechanisms can help reduce false positives by enabling the LOSTM model to assign lower weights to normal, non-Fraudulent transactions. This ensures that the model focuses on identifying genuine instances of Scam while minimizing false alarms.

4. CONCLUSION AND FUTURE ENHANCEMENT

Overall, aggregation and weightage mechanisms enhance the capabilities of LOSTM models by improving information integration, reducing noise, enabling selective attention, providing interpretability, and facilitating flexible and adaptive modeling. For payment card Scam detection, it is including capturing temporal dependencies, selective attention to suspicious transactions, handling imbalanced datasets, adapting to evolving Scam patterns, providing interpretability, and reducing false positives. These advantages contribute to more accurate and effective Scam detection systems, improving the security of payment card transactions and protecting cardholders from Fraudulent activities.

REFERENCES

1. Mathonsi, T., & van Zyl, T. L. (2022). A Statistics and Deep Learning Hybrid Method for Multivariate Time Series Forecasting and Mortality Modeling. Forecasting, 4(1), 1–25. https://doi.org/10.3390/forecast4010001
2. Ala'raj, M., Abbod, M. F., & Majdalawieh, M. (2021). Modelling customers PAYMENT CARD behaviour using bidirectional LOSTM neural networks. Journal of Big Data, 8(1). https://doi.org/10.1186/s40537-021-00461-7
3. Almuteer, A. H., Aloufi, A. A., Alrashidi, W. O., Alshobaili, J. F., & Ibrahim, D. M. (2021). Detecting PAYMENT CARD Scam using Machine Learning. International Journal of Interactive Mobile Technologies, 15(24), 108–122. https://doi.org/10.3991/IJIM.V15I24.27355
4. Tayeb, B., Amine, A., Reda, H. M., & Kumar, A. V. S. (2022). PAYMENT CARD Scam Detection Using Deep Learning Approach (LOSTM) Under IoT Environment. International Journal of Organizational and Collective Intelligence, 12(1), 1–20. https://doi.org/10.4018/ijoci.305207
5. S. V. S. S. Lakshmi, S. D. Kavilla "Machine Learning For PAYMENT CARD Scam Detection System", unpublished
6. N. Malini, Dr. M. Pushpa, "Analysis on PAYMENT CARD Scam Identification Techniques based on KNN and Outlier Detection", Advances in Electrical, Electronics, Information, Communication and BioInformatics (AEEICB), 2017 Third International Conference on pp. 255-258. IEEE.
7. Melo-Acosta, German E., et al. "Scam Detection in Big Data Using Supervised and Semi-Supervised Learning Techniques." 2017 IEEE Colombian Conference on Communications and Computing (COLCOM), 2017,doi:10.1109/colcomcon.2017.8088206.
8. http://www.rbi.org.in/Circular/CreditCard