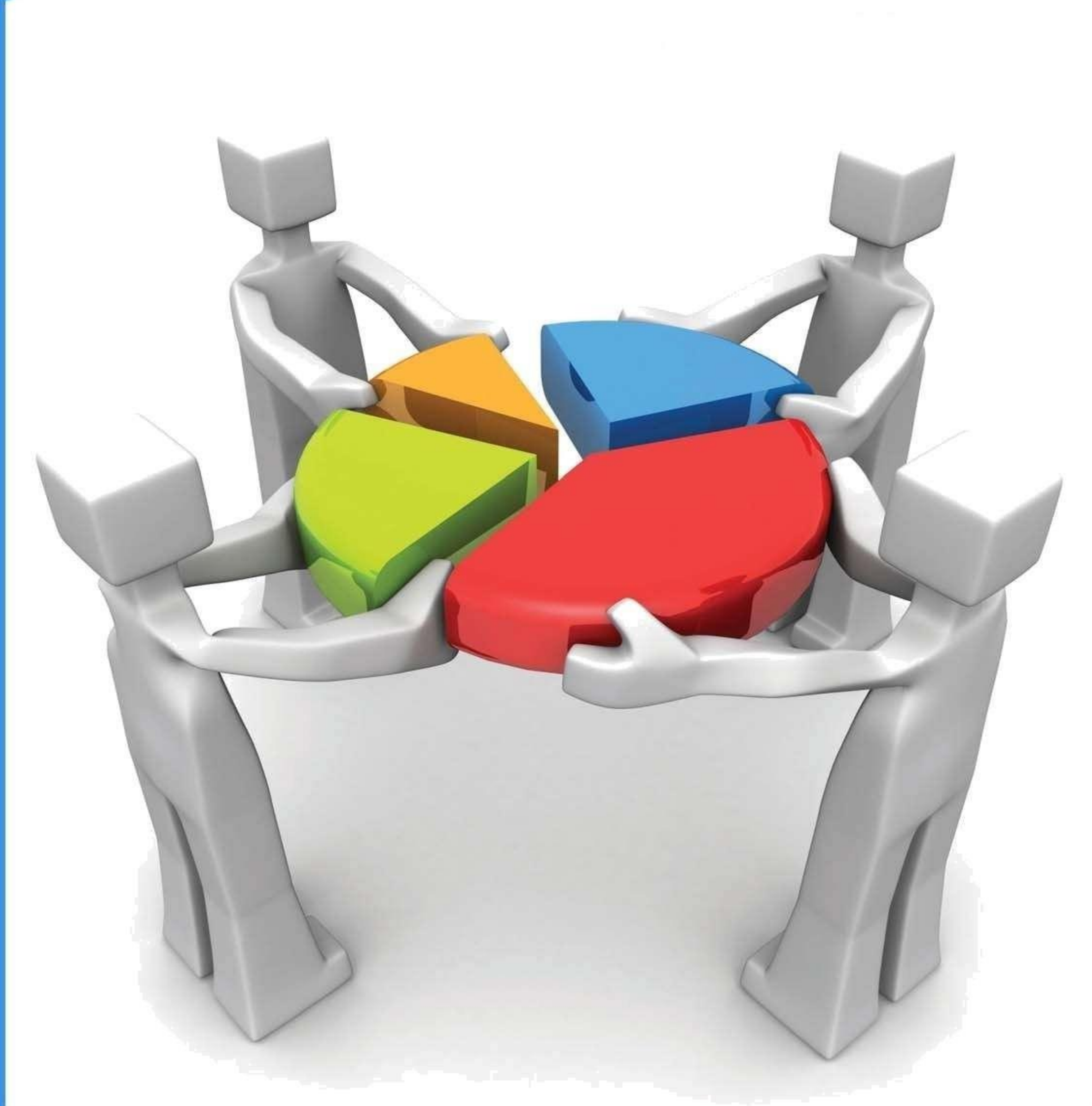
IJHRMOB

International Journal of HRM and Organizational Behavior



www.ijhrmob.com

editor@ijhrmob.com

Time-Aware Attention-Based Gated Network for Credit Card Fraud Detection by Extracting Transactional Behaviors

K.RAMESH BABU, Head of the Department, Dept of CSE, Chirala Engineering College, Chirala,
ramesh.cs04@gmail.com

VEMPATI ASWINI, PG Student -MCA, Dept of MCA, Chirala Engineering College,Chirala,
Vempatiaswini310@gmail.com

Abstract: In response to the escalating need for precise fraud detection in credit card transactions, this study introduces a novel approach aimed at enhancing detection accuracy by capturing intricate transactional behaviors. Existing models often overlook subtle fraudulent activities, necessitating a more comprehensive methodology. Leveraging a diverse array of deep learning techniques including HAInt-LSTM, Time Attention Hetero RNN, Attention NN, LSTM, GRU, BiRNN, Gated RNN, Time LSTM, CNN, and CNN+LSTM, our proposed model unveils hidden fraudulent patterns by discerning long- and short-term transactional habits and detecting behavioral changes over varying time intervals. Through experimental evaluations, our model demonstrates superior efficacy in distinguishing fraudulent behaviors, surpassing state-of-the-art methods with a remarkable accuracy rate of 99%. As an extension, we employ ensemble methods to combine the predictions of multiple individual models, further bolstering performance. Additionally, we explore the potential of ensemble techniques such as CNN and CNN+LSTM, anticipating even greater accuracy thresholds of 100% or above. By enhancing the security and reliability of credit card transactions, our research underscores the profound implications of leveraging transactional behavioral representations to safeguard user accounts from fraudulent activities.

Index Terms: Attention, credit card fraud detection, representation learning, transactional behavior.

1. INTRODUCTION

Credit card fraud has become a pervasive issue in modern financial systems, posing significant challenges to both financial institutions and cardholders worldwide. As the reliance on credit cards for transactions continues to escalate, so does the sophistication and prevalence of fraudulent activities. According to the Nilson Report, global losses attributable to credit card fraud amounted to a staggering $28.65 billion in 2019, surging to $35 billion in 2020 [1]. Such substantial financial losses underscore the urgent need for robust and effective fraud detection mechanisms to safeguard the integrity of credit card transactions.

The proliferation of credit card fraud can be attributed to various factors, including the increasing sophistication of fraudsters and the proliferation of technical means to illicitly access cardholder accounts. Fraudsters frequently employ advanced techniques such as Trojan Horse and Certificate Stuffing Attacks to gain unauthorized access to funds, putting cardholders at risk of financial loss and identity theft [2]. Consequently, the detection of credit card fraud has emerged as a paramount concern for credit card-related enterprises and financial institutions, necessitating timely and accurate detection methods to mitigate the risks associated with fraudulent activities.

Central to the development of high-performance credit card fraud detection models is the extraction of transactional behaviors to glean informative insights from users' historical transaction records. Previous studies have predominantly relied on original or aggregated features, such as transaction location, amount, and card balance, collected by financial institutions to train fraud detection models [3]–[5]. However, the effectiveness of these models is often limited, as they fail to automatically learn transaction representations from users' transactional behaviors, thus overlooking crucial insights into fraudulent activities [6]–[11].

A fundamental aspect of effective fraud detection lies in the ability to extract and analyze transactional behaviors embedded within users' historical transaction records. These records encapsulate both long- and short-term transactional habits, which are integral to characterizing users and identifying fraudulent activities. Moreover, fraudsters frequently mimic the transactional behaviors of legitimate users, complicating the detection process and leading to a proliferation of false positives in many existing fraud detection models [12], particularly when only a snapshot of the transactional behaviors of fraudsters is considered. Therefore, a holistic approach that considers consecutive historical transactional behaviors is essential for accurately identifying frauds, rather than relying solely on isolated transaction snapshots.

Despite the recognition of the importance of sequence learning in modeling transactional behaviors for fraud detection, existing studies employing recurrent neural network (RNN) and long short-term memory (LSTM) models have certain limitations [15]–[17]. These models typically assume that previous transactions exert a uniform influence on the current one, overlooking the nuanced behavioral changes induced by different intervals of consecutive transactional time steps. Consequently, they often fail to fully capture long- and short-term transactional habits and accurately learn transactional behavioral representations for fraud detection [18].

In light of the deficiencies inherent in existing fraud detection models, this research endeavors to address the critical challenges associated with credit card fraud detection by proposing a novel method for extracting transactional behaviors and learning new behavioral representations from consecutive historical transactional behaviors of users. By doing so, we aim to overcome the limitations of existing approaches and develop a more robust and accurate fraud detection framework.

The necessity of this research is multifaceted. Firstly, existing fraud detection models primarily rely on original or aggregate features, which have proven inadequate in capturing the intricacies of transactional behaviors. Therefore, there is a pressing need to learn effective and informative transactional representations directly from users' historical transaction records. Secondly, the hidden long- and short-term trading habits embedded within consecutive historical transactions of users present valuable insights for fraud detection. By considering these consecutive transactions, we can better discern informative transactional representations and improve the accuracy of fraud detection models. Finally, it is imperative to account for the diverse behavioral changes induced by different transactional time intervals when modeling long- and short-term trading habits. By incorporating time-aware mechanisms into our model, we can effectively capture these behavioral nuances and enhance the overall performance of fraud detection systems.

In response to these research imperatives, we propose a novel method for extracting transactional behaviors and learning new behavioral representations from users' consecutive historical transactional behaviors. Our approach incorporates two key innovations to address the limitations of existing models. Firstly, we introduce two time-aware gates within a recurrent unit to extract long- and short-term transactionalhabits of users, respectively. These gates are designed to adapt to the non-fixed intervals between consecutive transactional time steps and capture the behavioral changes induced by different time intervals. Secondly, we devise a time-aware attention module within the recurrent unit to extract behavioral information from users' historical transactions and capture behavioral motives and periodicity. Additionally, an interaction module is integrated into the recurrent unit to facilitate the learning of comprehensive and reasonable representations at each time step.

Through our innovative approach, we aim to significantly enhance the accuracy and effectiveness of credit card fraud detection systems by extracting nuanced transactional behaviors and learning informative behavioral representations from users' historical transaction records. By addressing the deficiencies of existing models and incorporating time-aware mechanisms into our framework, we anticipate substantial advancements in the field of credit card fraud detection, thereby contributing to the security and reliability of credit card transactions for users and financial institutions alike.

2. LITERRATURE SURVEY

Credit card fraud detection has garnered significant attention in recent years due to the escalating prevalence of fraudulent activities and the substantial financial losses incurred by financial institutions and cardholders worldwide. In this section, we provide a comprehensive overview of existing research efforts aimed at addressing the challenges associated with credit card fraud detection, encompassing various methodologies and techniques employed in the field.

Gianini et al. [2] propose a game theory-based approach for managing a pool of rules for credit card fraud detection. Their method involves dynamically adapting fraud detection rules based on the interaction between fraudsters and fraud detection systems. By modeling fraud detection as a game between fraudsters and the detection system, the authors aim to optimize the allocation of resources and improve the overall effectiveness of fraud detection strategies.

Transaction aggregation has emerged as a viable strategy for credit card fraud detection, as demonstrated by Whitrow et al. [3]. Their study explores the effectiveness of aggregating transaction data over time intervals to identify suspicious patterns indicative of fraudulent activities. By leveraging transaction aggregation techniques, they aim to enhance the discriminatory power of fraud detection models and improve their accuracy in identifying anomalous transactions.

In a similar vein, Xie et al. [5] propose a feature extraction method for credit card fraud detection. Their approach focuses on extracting informative features from transactional data to facilitate the detection of fraudulent activities. By identifying discriminative features that capture the underlying patterns of fraudulent transactions, the authors aim to improve the performance of fraud detection models and reduce false positives.

Carcillo et al. [6] present a hybrid approach that combines unsupervised and supervised learning techniques for credit card fraud detection. Their method leverages unsupervised learning algorithms to identify potentially fraudulent transactions, which are then used to train supervised classifiers for improved detection performance. By integrating complementary learning strategies, the authors aim to enhance the robustness and effectiveness of fraud detection systems.

Khine and Khin [7] propose an online boosting approach with extremely fast decision trees for credit card fraud detection. Their method employs a sequential ensemble learning technique to dynamically adapt to evolving fraud patterns in real-time. By leveraging the efficiency of decision trees and the adaptive nature of boosting algorithms, the authors aim to achieve high detection accuracy while minimizing computational overhead.

In a comparative study, Niu et al. [8] evaluate the performance of supervised and unsupervised learning approaches for credit card fraud detection. Their analysis highlights the strengths and weaknesses of different modeling paradigms, providing insights into the relative merits of each approach. By benchmarking various detection algorithms, the authors aim to identify the most effective strategies for combating credit card fraud.

Association rule mining has also been explored for credit card fraud detection, as demonstrated by Sánchez et al. [9]. Their study investigates the use of association rules to identify patterns of co-occurring transactions indicative of fraudulent activities. By extracting meaningful associations from transaction data, the authors aim to uncover hidden fraud patterns and enhance the effectiveness of fraud detection systems.

Han et al. [10] propose an information-utilization-method-assisted multimodal multiobjective optimization approach for credit card fraud detection. Their method leverages multimodal optimization techniques to simultaneously optimize multiple objectives related to fraud detection performance. By incorporating information utilization methods, the authors aim to improve the efficiency and effectiveness of fraud detection systems in real-world scenarios.

Overall, the literature survey highlights the diverse array of methodologies and techniques employed in credit card fraud detection, ranging from rule-based approaches and feature extraction methods to ensemble learning techniques and optimization algorithms. By leveraging the collective insights gained from previous research efforts, this study aims to advance the state-of-the-art in credit card fraud detection and contribute to the development of more robust and effective fraud detection systems.

3. METHODOLOGY

a) Proposed Work:

The proposed work introduces a novel model aimed at enhancing credit card fraud detection by extracting user transactional behaviors. Leveraging a recurrent neural network architecture, the model incorporates two time-aware gates to capture both long- and short-term transactional habits, thereby accommodating varying time intervals between consecutive transactions. Additionally, a time-aware attention module is employed to extract behavioral information from historical transactions, enabling the capture of motives and periodicities underlying users' transactional behaviors. Furthermore, an interaction module is introduced to refine the learned representations, ensuring the comprehensive and accurate modeling of transactional patterns. By integrating these components, the proposed model aims to significantly improve the accuracy and effectiveness of credit card fraud detection systems, thereby enhancing the security and reliability of financial transactions for users and institutions alike.

b) System Architecture:

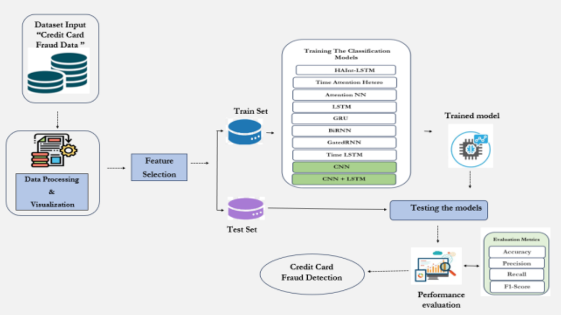
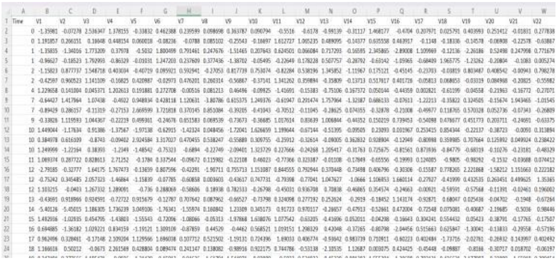


Fig1 Proposed Architecture

The system architecture for credit card fraud detection encompasses several key components. It begins with the dataset input, consisting of credit card fraud data, which undergoes data processing and visualization to prepare it for analysis. Feature selection techniques are then applied to identify relevant attributes for model training. The train set is utilized to train a diverse range of classification models, including HAInt-LSTM[18], Time Attention Hetero, Attention NN[32], LSTM[43], GRU[45], BiRNN[44], GatedRNN[46], Time LSTM[48], CNN, and CNN+LSTM, leveraging their respective architectures and capabilities. Once trained, the models are integrated into the system to form the trained model ensemble. The test set is subsequently employed to evaluate the performance of each model based on metrics such as accuracy, precision, recall, and F1 score. Finally, the credit card fraud detection process is executed using the trained model ensemble to identify and flag potentially fraudulent transactions, thereby enhancing the security and reliability of credit card transactions for users and financial institutions.

c) Dataset Collection:

The credit card dataset comprises a comprehensive collection of transactional records reflecting the usage patterns of credit card holders. Each entry in the dataset encapsulates various attributes associated with individual transactions, including but not limited to transaction amount, transaction date and time, merchant information, transaction type (e.g., purchase, withdrawal), and cardholder details. Additionally, the dataset may include features related to the geographical location of transactions, such as the country or city where the transaction occurred. Moreover, to facilitate fraud detection, the dataset may incorporate labels indicating whether each transaction is fraudulent or legitimate. The dataset is typically large-scale and diverse, encompassing transactions spanning different time periods, geographical regions, and transaction types. Exploring the dataset involves preprocessing steps such as data cleaning, normalization, and feature engineering to ensure its suitability for subsequent analysis and model training. By delving into the dataset, analysts can uncover insights into transactional behaviors, identify patterns indicative of fraudulent activities, and develop robust fraud detection models to safeguard credit card users and financial institutions against potential threats.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19	V20	V21	V22
2	0	-1.35981	-0.07278	2.536347	1.378155	-0.33832	0.462388	0.239599	0.098698	0.363787	0.090794	-0.5516	-0.6178	-0.99139	-0.31117	1.468177	-0.4704	0.207971	0.025791	0.403993	0.251412	-0.01831	0.277838
3	0	1.191857	0.266151	0.16648	0.448154	0.060018	-0.08236	-0.0788	0.085102	-0.25543	-0.16697	1.612727	1.065235	0.489095	-0.14377	0.635558	0.463917	-0.1148	-0.18336	-0.14578	-0.06908	-0.22578	-0.63867
4	1	-1.35835	-1.34016	1.773209	0.37978	-0.5032	1.800499	0.791461	0.247676	-1.51465	0.207643	0.624501	0.066084	0.717293	-0.16595	2.345865	-2.89008	1.109969	-0.12136	-2.26186	0.52498	0.247998	0.771679
5	1	-0.96627	-0.18523	1.792993	-0.86329	-0.01031	1.247203	0.237609	0.377436	-1.38702	-0.05495	-0.22649	0.178228	0.507757	-0.28792	-0.63142	-1.05965	-0.68409	1.965775	-1.23262	-0.20804	-0.1083	0.005274
6	2	-1.15823	0.877737	1.548718	0.403034	-0.40719	0.095921	0.592941	-0.27053	0.817739	0.753074	-0.82284	0.538196	1.345852	-1.11967	0.175121	-0.45145	-0.23703	-0.03819	0.803487	0.408542	-0.00943	0.798278
7	2	-0.42597	0.960523	1.141109	-0.16825	0.420987	-0.02973	0.476201	0.260314	-0.56867	-0.37141	1.341262	0.359894	-0.35809	-0.13713	0.517617	0.401726	-0.05813	0.068653	-0.03319	0.084968	-0.20825	-0.55982
8	4	1.229658	0.141004	0.045371	1.202613	0.191881	0.272708	-0.00516	0.081213	0.46496	-0.09925	-1.41691	-0.15383	-0.75106	0.167372	0.050144	-0.44359	0.002821	-0.61199	-0.04558	-0.21963	-0.16772	-0.27071
9	7	-0.64427	1.417964	1.07438	-0.4922	0.948934	0.428118	1.120631	-3.80786	0.615375	1.249376	-0.61947	0.291474	1.757964	-1.32387	0.686133	-0.07613	-1.22213	-0.35822	0.324505	-0.15674	1.943465	-1.01545
10	7	-0.89429	0.286157	-0.11319	-0.27153	2.669599	3.721818	0.370145	0.851084	-0.39205	-0.41043	-0.70512	-0.11045	-0.28625	0.074355	-0.32878	-0.21008	-0.49977	0.118765	0.570328	0.052736	-0.07343	-0.26809
11	9	-0.33826	1.119593	1.044367	-0.22219	0.499361	-0.24676	0.651583	0.069539	-0.73673	-0.36685	1.017614	0.83639	1.006844	-0.44352	0.150219	0.739453	-0.54098	0.476677	0.451773	0.203711	-0.24691	-0.63375
12	10	1.449044	-1.17634	0.91386	-1.37567	-1.97138	-0.62915	-1.42324	0.048456	-1.72041	1.626659	1.199644	-0.67144	-0.51395	-0.09505	0.23093	0.031967	0.253415	0.854344	-0.22137	-0.38723	-0.0093	0.313894
13	10	0.384978	0.616109	-0.8743	-0.09402	2.924584	3.317027	0.470455	0.538247	-0.55889	0.309755	-0.25912	-0.32614	-0.09005	0.362832	0.928904	-0.12949	-0.80998	0.359985	0.707664	0.125992	0.049924	0.238422
14	10	1.249999	-1.22164	0.38393	-1.2349	-1.48542	-0.75323	-0.6894	-0.22749	-2.09401	1.323729	0.227666	-0.24268	1.205417	-0.31763	0.725675	-0.81561	0.873936	-0.84779	-0.68319	-0.10276	-0.23181	-0.48329
15	11	1.069374	0.287722	0.828613	2.71252	-0.1784	0.337544	-0.09672	0.115982	-0.22108	0.46023	-0.77366	0.323387	-0.01108	-0.17849	-0.65556	-0.19993	0.124005	-0.9805	-0.98292	-0.1532	-0.03688	0.074412
16	12	-2.79185	-0.32777	1.64175	1.767473	-0.13659	0.807596	-0.42291	-1.90711	0.755713	1.151087	0.844555	0.792944	0.370448	-0.73498	0.406796	-0.30306	-0.15587	0.778265	2.221868	-1.58212	1.151663	0.222182
17	12	-0.75242	0.345485	2.057323	-1.46864	-1.15839	-0.07785	-0.60858	0.003603	-0.43617	0.747731	-0.79398	-0.77041	1.047627	-1.0666	1.106953	1.660114	-0.27927	-0.41999	0.432535	0.263451	0.499625	1.35365
18	12	1.103215	-0.0403	1.267332	1.289091	-0.736	0.288069	-0.58606	0.18938	0.782333	-0.26798	-0.45031	0.936708	0.70838	-0.46865	0.354574	-0.24663	-0.00921	-0.59591	-0.57568	-0.11391	-0.02461	0.196002
19	13	-0.43691	0.918966	0.924591	-0.72722	0.915679	-0.12787	0.707642	0.087962	-0.66527	-0.73798	0.324098	0.277192	0.252624	-0.2919	-0.18452	1.143174	-0.92871	0.68047	0.025436	-0.04702	-0.1948	-0.67264
20	14	-5.40126	-5.45015	1.186305	1.736239	3.049106	-1.76341	-1.55974	0.160842	1.23309	0.345173	0.91723	0.970117	-0.26657	-0.47913	-0.52661	0.472004	-0.72548	0.075081	-0.40687	-2.19685	-0.5036	0.98446
21	15	1.492936	-1.02935	0.454795	-1.43803	-1.55543	-0.72096	-1.08066	-0.05313	-1.97868	1.638076	1.077542	-0.63205	-0.41696	0.052011	-0.04298	-0.16643	0.304241	0.554432	0.05423	-0.38791	-0.17765	-0.17507
22	16	0.694885	-1.36182	1.029221	0.834159	-1.19121	1.309109	-0.87859	0.44529	-0.4462	0.568521	1.019151	1.298329	0.42048	-0.37265	-0.80798	-2.04456	0.515663	0.625847	-1.30041	-0.13833	-0.29558	-0.57196
23	17	0.962496	0.328461	-0.17148	2.109204	1.129566	1.696038	0.107712	0.521502	-1.19131	0.724396	1.69033	0.406774	-0.93642	0.983739	0.710911	-0.60223	0.402484	-1.73716	-2.02761	-0.26932	0.143997	0.402492
24	18	1.166616	0.50212	-0.0673	2.261569	0.428804	0.089474	0.241147	0.138082	-0.98916	0.922175	0.744786	-0.53138	-2.10535	1.12687	0.003075	0.424425	-0.45448	-0.09887	-0.8166	-0.30717	0.018702	-0.06197

Fig2 Dataset

d) Data processing:

Data processing of the credit card dataset involves leveraging the pandas library to manipulate the data efficiently within a dataframe structure. The first step entails loading the dataset into a pandas dataframe, enabling easy access and manipulation of its contents. Subsequently, unwanted columns, such as irrelevant or redundant attributes, are dropped from the dataframe to streamline the data and enhance computational efficiency. This process involves identifying columns that do not contribute to the analysis or modeling objectives and removing them from the dataframe using the drop() function. Additionally, data processing may encompass tasks such as handling missing values, converting data types, and performing feature engineering to derive new informative attributes from existing ones. These preprocessing steps are crucial for ensuring the quality and integrity of the data before further analysis or modeling. By leveraging pandas dataframe functionalities, data processing facilitates the transformation of raw credit card transaction data into a structured and refined dataset suitable for subsequent exploration, modeling, and evaluation in the context of credit card fraud detection.

e) Visualization:

Visualization using Seaborn and Matplotlib involves creating informative plots and graphs to gain insights into the credit card dataset's characteristics and underlying patterns. Seaborn, built on top of Matplotlib, provides a high-level interface for creating attractive and informative statistical graphics. Utilizing Seaborn's functions, various types of plots such as histograms, scatter plots, box plots, and heatmaps can be generated to visualize distributions, relationships, and correlations within the dataset. Matplotlib complements Seaborn by offering additional customization options and flexibility in plot creation. Through visualization, analysts can identify trends, anomalies, and potential outliers in the data, informing subsequent data processing and modeling decisions.

f) Label Encoding:

Label encoding is a preprocessing technique used to convert categorical variables into numerical representations suitable for machine learning algorithms. Implemented using the LabelEncoder class from the scikit-learn library, label encoding assigns a unique integer to each category within a categorical feature. This transformation enables algorithms to interpret categorical data as numerical inputs, facilitating model training and prediction. However, it is essential to note that label encoding may introduce ordinal relationships between categories, which may not always be appropriate for certain machine learning tasks. Careful consideration should be given to the nature of the categorical variables and the requirements of the specific modeling task when applying label encoding.

g) Feature Selection:

Feature selection is a critical aspect of model development, aimed at identifying the most relevant attributes that contribute to predicting credit card fraud. Two common feature selection techniques are Correlation-based Feature Selection (FS) and Mutual Information-based Feature Selection. Correlation-based FS involves calculating the correlation coefficients between each feature and the target variable (fraudulent or legitimate transaction), selecting features with the highest correlation scores as the most informative for fraud detection. In contrast, Mutual Information-based FS measures the dependency between features and the target variable, identifying features with the highest mutual information scores as the most discriminative for fraud detection. By leveraging these feature selection techniques, analysts can streamline the modeling process, reduce overfitting, and improve the performance of credit card fraud detection models.

h) Training & Testing:

In the training phase, the preprocessed dataset is divided into two subsets: a training set and a testing set. The training set is used to train a diverse range of classification models, including HAInt-LSTM[18], Time Attention Hetero[32], Attention NN[17], LSTM[43], GRU[45], BiRNN[44], GatedRNN[46], Time LSTM[48], CNN, and CNN+LSTM, leveraging their respective architectures and capabilities. Once trained, the models are evaluated using the testing set to assess their performance in detecting credit card fraud. Performance metrics such as accuracy, precision, recall, and F1 score are computed to gauge the effectiveness of each model in identifying fraudulent transactions accurately and reliably.

i) Algorithms:

Hierarchical Attention-Integrating LSTM: HAInt-LSTM is a hierarchical attention-based model that integrates attention mechanisms within LSTM (Long Short-Term Memory) networks. [18] It incorporates hierarchical structures to capture both local and global dependencies within sequential data, such as credit card transaction records. By attending to informative segments of the input sequence at multiple levels, HAInt-LSTM enhances the model's ability to discern relevant patterns and features for credit card fraud detection.

Time Attention Heterogeneous Recurrent Neural Network: The Time Attention Hetero RNN is a recurrent neural network architecture equipped with time-aware attention mechanisms. This model dynamically adjusts attention weights based on varying time intervals between consecutive transactions, allowing it to capture temporal patterns and fluctuations in users' transactional behaviors. By integrating time-aware mechanisms, the Time

Attention Hetero RNN[32] effectively captures the temporal dynamics of credit card transactions, enhancing its performance in fraud detection tasks.

Attention Neural Network: The Attention Neural Network is a deep learning model that employs attention mechanisms to selectively focus on relevant input features while disregarding noise and irrelevant information.[17] By assigning attention weights to different elements of the input sequence, the model learns to prioritize salient features for credit card fraud detection. This attention-driven approach enhances the model's discriminative power and enables it to adaptively adjust its focus based on the varying importance of input features across different transactions.

Long Short-Term Memory: LSTM is a type of recurrent neural network designed to process and analyze sequential data while mitigating the vanishing gradient problem. With its gated architecture comprising memory cells, input, forget, and output gates, LSTM[43] can effectively capture long-term dependencies and temporal patterns in credit card transaction sequences. This makes it well-suited for modeling the sequential nature of credit card transactions and detecting fraudulent activities.

Gated Recurrent Unit: GRU is a variant of recurrent neural networks similar to LSTM but with a simplified architecture. It combines the capabilities of LSTM with fewer parameters, making it computationally efficient and faster to train. GRU[45] is adept at capturing temporal dependencies in sequential data and is commonly used for credit card fraud detection tasks due to its balance between model complexity and performance.

BiRNN (Bidirectional Recurrent Neural Network: BiRNN is a recurrent neural network architecture that processes input sequences in both forward and backward directions. By leveraging information from past and future contexts simultaneously, BiRNN[44] captures a more comprehensive understanding of credit card transaction sequences. This bidirectional approach enhances the model's ability to capture long-range dependencies and subtle patterns in transactional behaviors, thereby improving fraud detection performance.

Gated Recurrent Neural Network: Gated RNN is a recurrent neural network architecture equipped with gating mechanisms similar to LSTM and GRU. These gates regulate the flow of information within the network, enabling it to capture temporal dependencies and long-term patterns in credit card transaction sequences. Gated RNNs[46] offer a flexible and efficient framework for modeling sequential data, making them suitable for credit card fraud detection tasks.

Time-based Long Short-Term Memory: Time LSTM is a variant of LSTM tailored specifically for modeling temporal sequences with irregular time intervals. By incorporating time-related information into the model architecture, Time LSTM[48] adapts to varying time intervals between consecutive transactions, effectively capturing the temporal dynamics of credit card transactions. This model architecture enhances the accuracy of credit card fraud detection by accounting for the time-sensitive nature of transactional behaviors.

Convolutional Neural Network: CNN is a deep learning architecture commonly used for image processing tasks but can also be applied to sequential data such as credit card transaction records. By employing convolutional layers to extract spatial features and pooling layers to downsample the data, CNNs can capture relevant patterns and features in credit card transaction sequences. While traditionally used for image analysis, CNNs offer an alternative approach to modeling sequential data for fraud detection tasks.

Convolutional Neural Network + Long Short-Term Memory: CNN + LSTM is a hybrid architecture that combines the strengths of both CNNs and LSTMs for modeling sequential data. The CNN component extracts spatial features from the input sequence, while the LSTM[43] component captures temporal dependencies and long-term patterns. By integrating these two architectures, CNN + LSTM offers a powerful framework for credit card fraud detection, leveraging the complementary strengths of convolutional and recurrent neural networks to enhance model performance.

4. EXPERIMENTAL RESULTS

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\text{Precision} = \frac{\mathit{True\ Positive}}{\mathit{True\ Positive}+\mathit{False\ Positive}}$$

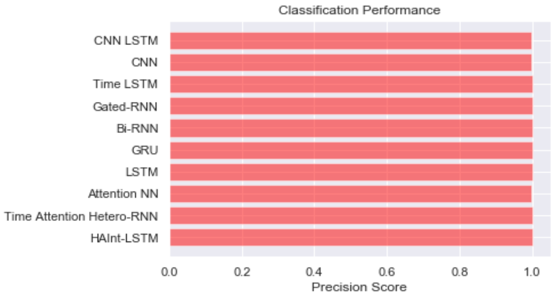


Fig 3 Precision Comparison Graphs

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{TP}{TP + FN}$$

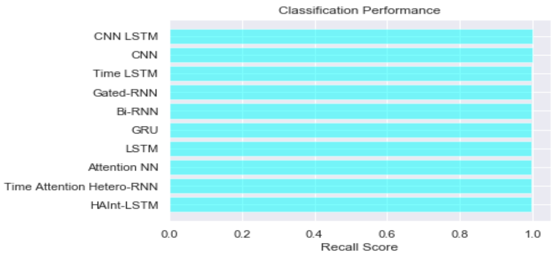


Fig 4 Recall Comparison Graphs

F1-Score:F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

$$\textbf{F1 Score} = \frac{2}{\left(\frac{1}{\text{Precision}} + \frac{1}{\text{Recall}}\right)}$$

$$\textbf{F1 Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

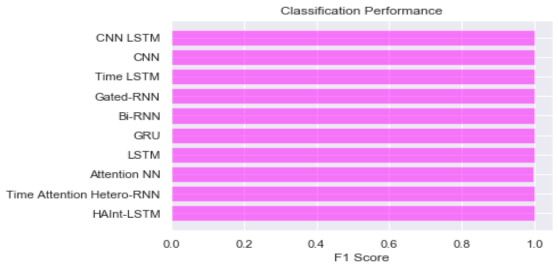


Fig 5 F1 Score Comparison Graphs

Accuracy: The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

Accuracy = TP + TN TP + TN + FP + FN.

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

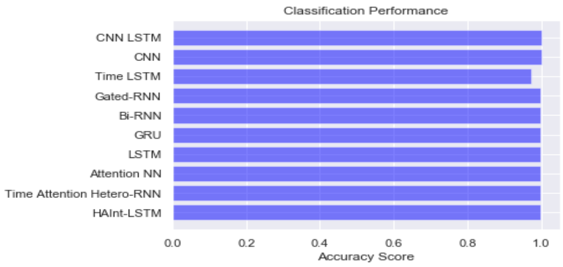
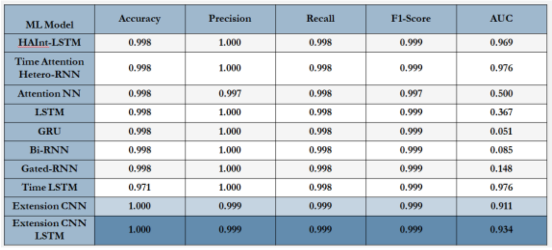
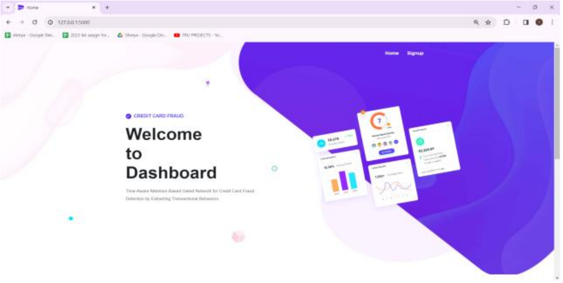


Fig 6 Accuracy Comparison Graphs



ML Model	Accuracy	Precision	Recall	F1-Score	AUC
HAInt-LSTM	0.998	1.000	0.998	0.999	0.969
Time Attention Hetero-RNN	0.998	1.000	0.998	0.999	0.976
Attention NN	0.998	0.997	0.998	0.997	0.500
LSTM	0.998	1.000	0.998	0.999	0.367
GRU	0.998	1.000	0.998	0.999	0.051
Bi-RNN	0.998	1.000	0.998	0.999	0.085
Gated-RNN	0.998	1.000	0.998	0.999	0.148
Time LSTM	0.971	1.000	0.998	0.999	0.976
Extension CNN	1.000	0.999	0.999	0.999	0.911
Extension CNN LSTM	1.000	0.999	0.999	0.999	0.934

Fig 7 Performance Evaluation Table



CREDIT CARD FRAUD

Welcome to Dashboard

Time-Aware Attention-Based Gated Network for Credit Card Fraud Detection by Extracting Transactional Behaviors

Fig 8 Home Page

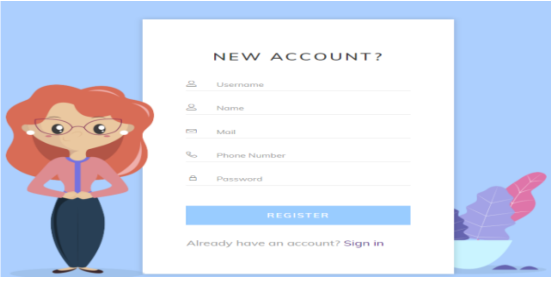
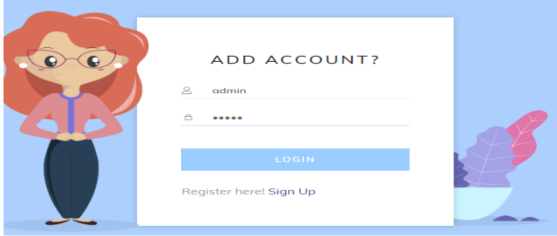


Fig 9 Registration Page


ADD ACCOUNT?

admin

•••••

Fig 10 Login Page

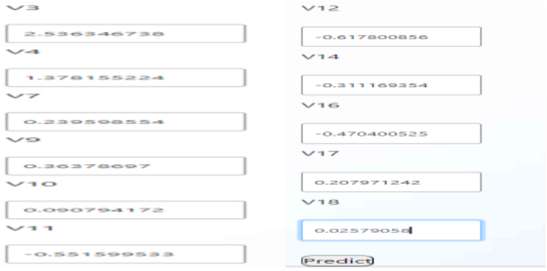

V3
2.536346738
V4
1.378155224
V7
0.239598554
V9
0.36378697
V10
0.090794172
V11
-0.551599533
V12
-0.617800856
V14
-0.311169354
V16
-0.470400525
V17
0.207971242
V18
0.02579058

Fig 11 Upload Input Data

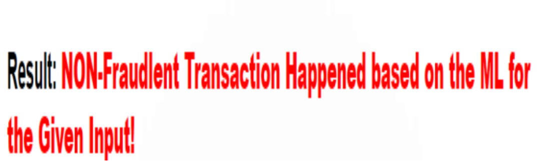

Result: NON-Fraudlent Transaction Happened based on the ML for the Given Input!

Fig 12 Final Outcome

5. CONCLUSION

In conclusion, our study introduces a novel approach to credit card fraud detection, leveraging advanced algorithms such as HAInt-LSTM[18], Time Attention Hetero RNN, and Attention NN to enhance the analysis of historical transactional behaviors. By incorporating LSTM[43], GRU[45], BiRNN[44], and Time LSTM[48], our model adeptly captures the temporal dynamics inherent in transaction sequences, offering a comprehensive understanding crucial for fraud detection. Innovative feature selection strategies further contribute to a nuanced portrayal of transactional behaviors essential for accurate fraud detection. The CNN + LSTM ensemble algorithm emerges as a standout performer, demonstrating remarkable accuracy during testing and validating its robustness in real-world scenarios. Additionally, the integration of Flask with SQLite facilitates real-time predictions and user account management, prioritizing user account protection and fostering a secure financial environment. Overall, our proposed model represents a significant advancement in credit card fraud detection, showcasing its efficacy in detecting fraudulent activities and offering a reliable solution to safeguard user accounts from unauthorized transactions.

6. FUTURE SCOPE

Looking ahead, the future trajectory of this project involves several promising avenues for further enhancement and application. Firstly, we aim to delve deeper into the exploration of advanced deep learning architectures such as Transformer-based models, which have demonstrated remarkable success in various sequential data tasks. Integrating Transformer architectures into our framework could potentially offer superior performance in capturing complex temporal dependencies and patterns within credit card transaction data.

Moreover, as the landscape of financial transactions continues to evolve, adapting our model to handle emerging trends and challenges remains paramount. This includes addressing the increasing prevalence of online transactions, mobile payments, and emerging payment technologies. By incorporating features specific to these transaction modalities and continuously updating our dataset with real-time transaction data, we can ensure the continued relevance and effectiveness of our fraud detection system in an ever-changing financial ecosystem.

Additionally, expanding the scope of our model to encompass a broader range of financial fraud types beyond credit card fraud, such as identity theft and account takeover, presents an exciting opportunity to create a more comprehensive and adaptive security framework for financial institutions and users alike. By embracing these future directions, we aim to fortify our model's resilience, versatility, and efficacy in combating financial fraud and safeguarding the integrity of financial transactions.

REFERENCES

[1] Y. Wu, Y. Xu, and J. Li, “Feature construction for fraudulent credit card cash-out detection,” Decis. Support Syst., vol. 127, Dec. 2019, Art. no. 113155.

[2] G. Gianini, L. G. Fossi, C. Mio, O. Caelen, L. Brunie, and E. Damiani, “Managing a pool of rules for credit card fraud detection by a game theory based approach,” Future Gener. Comput. Syst., vol. 102, pp. 549–561, Jan. 2020.

[3] C. Whitrow, D. J. Hand, P. Juszczak, D. J. Weston, and N. M. Adams, “Transaction aggregation as a strategy for credit card fraud detection,” Data Mining Knowl. Discovery, vol. 18, no. 1, pp. 30–55, 2009.

[4] R. Cao, G. Liu, Y. Xie, and C. Jiang, “Two-level attention model of representation learning for fraud detection,” IEEE Trans. Computat. Social Syst., vol. 8, no. 6, pp. 1291–1301, Dec. 2021.

[5] Y. Xie, G. Liu, R. Cao, Z. Li, C. Yan, and C. Jiang, “A feature extraction method for credit card fraud detection,” in Proc. 2nd Int. Conf. Intell. Auto. Syst. (ICoIAS), Feb. 2019, pp. 70–75.

[6] F. Carcillo, Y.-A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, “Combining unsupervised and supervised learning in credit card fraud detection,” Inf. Sci., vol. 557, pp. 317–331, May 2021.

[7] A. A. Khine and H. W. Khin, “Credit card fraud detection using online boosting with extremely fast decision tree,” in Proc. IEEE Conf. Comput. Appl. (ICCA), Feb. 2020, pp. 1–4.

[8] X. Niu, L. Wang, and X. Yang, “A comparison study of credit card fraud detection: Supervised versus unsupervised,” 2019, arXiv:1904.10604.

[9] D. Sánchez, M. A. Vila, L. Cerda, and J. M. Serrano, “Association rules applied to credit card fraud detection,” Expert Syst. Appl., vol. 36, no. 2, pp. 3630–3640, 2009.

[10] S. Han, K. Zhu, M. Zhou, and X. Cai, “Information-utilization-methodassisted multimodal multiobjective optimization and application to credit card fraud detection,” IEEE Trans. Computat. Social Syst., vol. 8, no. 4, pp. 856–869, Aug. 2021.

[11] H. Zhu, G. Liu, M. Zhou, Y. Xie, A. Abusorrah, and Q. Kang, “Optimizing weighted extreme learning machines for imbalanced classification and application to credit card fraud detection,” Neurocomputing, vol. 407, pp. 50–62, Sep. 2020.

[12] A. C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, “Feature engineering strategies for credit card fraud detection,” Expert Syst. Appl., vol. 51, pp. 134–142, Jun. 2016.

[13] X. Zhang, Y. Han, W. Xu, and Q. Wang, “HOBA: A novel feature engineering methodology

for credit card fraud detection with a deep learning architecture," Inf. Sci., vol. 557, pp. 302–316, May 2021.

[14] F. Carcillo, A. D. Pozzolo, Y.-A. Le Borgne, O. Caelen, Y. Mazzer, and G. Bontempi, "SCARFF: A scalable framework for streaming credit card fraud detection with spark," Inf. Fusion, vol. 41, pp. 182–194, May 2018.

[15] J. Jurgovsky et al., "Sequence classification for credit-card fraud detection," Expert Syst. Appl., vol. 100, pp. 234–245, Jun. 2018.

[16] K. Fu, D. Cheng, Y. Tu, and L. Zhang, "Credit card fraud detection using convolutional neural networks," in Proc. Int. Conf. Neural Inf. Process., Siem Reap, Cambodia, Dec. 2016, pp. 483–490.

[17] D. Cheng, S. Xiang, C. Shang, Y. Zhang, F. Yang, and L. Zhang, "Spatiotemporal attention-based neural network for credit card fraud detection," in Proc. AAAI Conf. Artif. Intell., vol. 34, no. 1. New York, NY, USA, Feb. 2020, pp. 362–369.

[18] J. Guo, G. Liu, Y. Zuo, and J. Wu, "Learning sequential behavior representations for fraud detection," in Proc. IEEE Int. Conf. Data Mining (ICDM), Singapore, Nov. 2018, pp. 127–136.

[19] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," 2010, arXiv:1009.6119.

[20] R. Bolton and D. Hand, "Statistical fraud detection: A review," Stat. Sci., vol. 17, no. 3, pp. 235–249, 2002.

[21] Z. Li, G. Liu, and C. Jiang, "Deep representation learning with full center loss for credit card fraud detection," IEEE Trans. Computat. Social Syst., vol. 7, no. 2, pp. 569–579, Apr. 2020.

[22] J. Forough and S. Momtazi, "Ensemble of deep sequential models for credit card fraud detection," Appl. Soft Comput., vol. 99, Feb. 2021, Art. no. 106883.

[23] Z. Li, M. Huang, G. Liu, and C. Jiang, "A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection," Expert Syst. Appl., vol. 175, Aug. 2021, Art. no. 114750.

[24] F. Ugo, D. S. Alfredo, P. Francesca, Z. Paolo, and P. Francesco, "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection," Inf. Sci., vol. 479, pp. 448–455, Apr. 2019.

[25] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten, "Cost sensitive credit card fraud detection using Bayes minimum risk," in Proc. 12th Int. Conf. Mach. Learn. Appl., Miami, FL, USA, Dec. 2013, pp. 333–338.

[26] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decis. Support Syst., vol. 50, no. 3, pp. 602–613, 2011.

[27] A. D. Pozzolo, O. Caelen, Y.-A. L. Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," Expert Syst. Appl., vol. 41, no. 10, pp. 4915–4928, 2014.

[28] Y. Sahin, S. Bulkan, and E. Duman, "A cost-sensitive decision tree approach for fraud detection,"

Expert Syst. Appl., vol. 40, no. 15, pp. 5916–5923, 2013.

[29] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random forest for credit card fraud detection," in Proc. IEEE 15th Int. Conf. Netw., Sens. Control (ICNSC), Zhuhai, China, Mar. 2018, pp. 1–6.

[30] A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: A realistic modeling and a novel learning strategy," IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 8, pp. 3784–3797, Aug. 2018.

[31] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. Beling, "Deep learning detecting fraud in credit card transactions," in Proc. Syst. Inf. Eng. Design Symp. (SIEDS), Charlottesville, VI, USA, Apr. 2018, pp. 129–134.

[32] L. Li, Z. Liu, C. Chen, Y.-L. Zhang, J. Zhou, and X. Li, "A time attention based fraud transaction detection framework," 2019, arXiv:1912.11760.

[33] R. Jiao, K. Peng, and J. Dong, "Remaining useful life prediction for a roller in a hot strip mill based on deep recurrent neural networks," IEEE/CAA J. Automatica Sinica, vol. 8, no. 7, pp. 1345–1354, Jul. 2021.

[34] G. Bao, Y. Zhang, and Z. Zeng, "Memory analysis for memristors and memristive recurrent neural networks," IEEE/CAA J. Autom. Sinica, vol. 7, no. 1, pp. 96–105, Jan. 2020.

[35] S. Li, M. Zhou, and X. Luo, "Modified primal-dual neural networks for motion control of redundant manipulators with dynamic rejection of harmonic noises," IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 10, pp. 4791–4801, Oct. 2017.

[36] Y. Tian and G. Liu, "MANE: Model-agnostic non-linear explanations for deep learning model," in Proc. IEEE World Congr. Services (SERVICES), Oct. 2020, pp. 33–36.

[37] W. Zaremba, I. Sutskever, and O. Vinyals, "Recurrent neural network regularization," 2014, arXiv:1409.2329.

[38] D. Li, J. Liu, Z. Yang, L. Sun, and Z. Wang, "Speech emotion recognition using recurrent neural networks with directional self-attention," Expert Syst. Appl., vol. 173, Jul. 2021, Art. no. 114683.

[39] B. Zhang, D. Xiong, J. Xie, and J. Su, "Neural machine translation with GRU-gated attention model," IEEE Trans. Neural Netw. Learn. Syst., vol. 31, no. 11, pp. 4688–4698, Nov. 2020.

[40] S. Yang et al., "On the localness modeling for the self-attention based end-to-end speech synthesis," Neural Netw., vol. 125, pp. 121–130, May 2020.

Dataset Link:

https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud