Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 4 Issue 3 (2024)

A Novel Fraud Detection System based on Intrusion Detection for E-Commerce applications Using Neural Network Models

Dr B. Amarnath Reddy,
Assistant Professor, Department of Finance and Marketing, Vignana Jyothi Institute of Management, Hyderabad, India. amarnathreddy.b6@gmail.com

Dr Daniel Pilli,
Assistant Professor, Department of MBA, KL Business School, Koneru Lakshmaiah Educational Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India, danielpilli@kluniversity.in

Dr K. Suresh Kumar,
Professor, Department of MBA, Panimalar Engineering College, Chennai, Tamilnadu, India. pecmba19@gmail.com

Dr E. Manigandan,
Associate Professor, Department of Information Technology, School of Business, Galgotias University, Greater Noida, Uttar Pradesh, India. ibmmani78@gmail.com

Ujwal Prakash,
Assistant Professor, Department of Management, Arka Jain University, Mohanpur, Jharkhand, India. ujwal.prakas@gmail.com

Dr M. S. Kuttimarks,
Associate Professor, Civil Department, SSJCET, Asangaon, Thane, Maharashtra, India. drkuttimarks.ssjcet@gmail.com

Abstract –The idea of using the Internet to trade goods and services has grown in popularity at an exponential rate. Because of the Internet, online transactions have advanced significantly, removing the limitations of physical locations and currencies. The anonymity of the Internet, however, does not make it a perfect place for paying for things. With the rise of online transactions has come an equal and opposite rise in the frequency of assaults targeting the safety of online systems. Fraudulent transactions on auction sites and e-commerce online applications have been getting worse recently. Some of these fraudulent e-commerce transactions are the result of actual hacks into these websites. Unfortunately, despite widespread knowledge of these facts, no workable solution to the issue of application-based attacks in e-commerce has been found as of yet.

Keywords—Fraud Detection System, Intrusion Detection, convolutional Neural Network (CNN).

I. INTRODUCTION

Online shopping apps are frequently the target of attacks. Coincident with the proliferation of new types of fraud like computer penetration and mobile phone fraud, the prevalence of more traditional types of fraud like money laundering has also increased. The first concern should be the complete and total eradication of fraud. New protocols are necessary to protect customers from imposters that conduct fraud. Usually, these steps are grouped into two main categories: fraud detection and fraud prevention. Eliminating potential points of fraud is the main objective of fraud prevention. First and first, prevention should be the goal when it comes to safeguarding against fraud[1]. There are a plethora of fraud prevention solutions that may be integrated with e-commerce platforms. Some examples include credit card transaction security systems, passwords, and tokens. On the other hand, when fraud prevention fails because of system errors, fraud detection becomes essential. Cowardly customers and directors re-learn by teach from the everyday struggles of the security supervisory groups to keep their skills up-to-date with the latest vulnerabilities, viruses, and breaks. Organization access systems are a terrific resource for security-minded directors and executives when it comes to deciding on information technology strategy. The prevalence of invasions

necessitates the installation of Intrusion Detection Systems (IDS) to forestall their occurrence[2]. One kind of security software is known as IDS, and its purpose is to notify administrators if there is an attempt to breach the data framework in an unauthorized or destructive manner. Customers' lives have been greatly simplified by the proliferation of internet banking services, mobile banking, and telephone banks. They offer a more pleasant, easy, and convenient alternative for businesses. Users of online financial services, conversely, are understandably concerned about safety[3]. The rise of online transactions has provided con artists with a fertile environment for their ever-evolving schemes. When customers lose money due to a fraudulent transaction, they lose faith in the security of the online banking system. The growth and development of online trade have been phenomenal in recent years. Thanks to advancements in communication technology, e-commerce platforms, and digital transformation, more and more people are opting to shop online. Businesses and consumers alike can reap several benefits from e-commerce platforms[4]. Take, for instance, how it simplifies buying, reduces costs, and grants clients greater payment flexibility by enabling them to compare pricing and product quality. The exponential growth of e-commerce platforms and the corresponding increase in transaction volumes have, unsurprisingly, been accompanied by an increase in fraud incidents. Criminals stand to collect a substantial amount of money from exploiting security holes in electronic payment systems. Therefore, strong and smart fraud detection systems need to be set up to prevent these financial and economic losses. One of the most basic ways to spot fraud is to search for patterns in customer data that can point to deceit. The most important pieces of data evaluated are customers' payment histories, previous behaviors, and internet navigation trails.

II. Literature Survey

Online Store Monitoring in Real-Time In order to ensure the security of online transactions, real-time monitoring is crucial. In their work, the authors stressed the importance of real-time monitoring to detect and handle security events in e-commerce systems. The importance of monitoring user actions, network traffic, and system records for signs of unusual activity is emphasized. In [5], the authors proposed an intrusion prevention system for online marketplaces that relies on Deep Learning (DL) algorithms and operates in real time. With the help of a Long Short Term Memory (LSTM) neural network, they examined network traffic in search of suspicious behaviors. In a related work, they introduced a real-time intrusion prevention system for e-commerce platforms that combined signature-based and behavior-based detection techniques, much like [6]. The proposed approach achieved a detection rate of 98.8%. The authors of [7] proposed a real-time intrusion prevention solution for e-commerce platforms using a Support Vector Machine (SVM) algorithm. A whopping 99.2% of the time, the proposed system was spot on. The use of DL algorithms to provide real-time protection for e-commerce systems was proposed in a recent study. They used a Deep Belief Network (DBN) to detect malicious activities in network traffic. A 99.4% success rate was achieved using the proposed method, in agreement with [8]. There are numerous possible reasons why online applications could be attacked, including coding faults, design flaws, configuration errors, and validation errors that include user input. In [9], the authors proposed an intrusion prevention system that relies on Machine Learning (ML) algorithms and operates in real-time. They used Decision Tree (DT) approaches, Naïve Bayes (NB), and SVM to analyze the network data and find malicious actions. A staggering 98.8% detection rate was achieved using the proposed method. In their presentation of a real-time intrusion prevention system, the authors of [10] used DL algorithms. The proposed technique used a Convolutional Neural Network (CNN) to detect malicious activities in network traffic. A staggering 99.5 percent detection rate was achieved by the proposed approach. [11] used SVM and Random Forests (RF) to find industrial data anomalies that indicated intrusions. Investigates using SVMs and RF to discover anomalies in industrial data. This study suggests that combining SVM with supplementary methods could revolutionize e-commerce user behaviour anomaly detection. Use older ML approaches with newer ones to detect suspicious trends in network data [12]. This method combines ML technologies to improve anomaly detection accuracy and resilience. Even in non-e-commerce settings, combining algorithms to boost detection performance can help you improve your SVM-based system. A technique that combines Bayesian Network (BN) approaches with (SVM) is presented by the authors of [13] for the purpose of finding outliers. This study's findings might provide light on state-of-the-art approaches to enhancing SVM-based anomaly detection systems. Knowing how to integrate Bayesian models with SVM could help an anomaly detection algorithm in a future upgrade effort. In [14] assess how well Multi-Layer Artificial Neural Network (ML-ANN) (as parts of DL topologies) detect fraud. LSTM, parameter changes, and other memory and time components are part of these networks. In [15], classifiers from supervised BN such as NB, K2, logistics, J48, and Tree Augmented Naïve Bayes (TAN) are utilized. In comparison to scores acquired prior to this step, all of the classifiers achieve an accuracy rate of more than 95.2 percent once the dataset is preprocessed using Principal Component Analysis (PCA) and normalization. Filtered data significantly improves the performance of every Bayesian classifier (BC). In [16] [17], they used a combination of resampling techniques and predictive models including logistic regression (LR),

XGBoost, and RF to determine if a transaction is valid or not. When used in combination with other models, the most successful resampling approach is a combination of the Tomek Link elimination and the Synthetic Minority Over-Sampling Technique (SMOTE) using a RF algorithm. To identify anomalies in online payment systems, [18] proposed a Continuous Progressive Neural Networks GA (CPNN-GA) hybrid method. This approach uses genetic algorithm (GA) and ANN parameters. High fraud detection rates with minimal false alarm rates are the target, together with optimal solution quality in terms of classification. Experimental results show that CPPN has an accuracy of 84.43, GA of 89.43, and a total hit rate of 97.18 when the two methods are combined. [19] The researchers examined many ML algorithms. Based on the results, RF provided the best accurate fraud classification at 99.95%, followed by LR at 97.45%, and NB at 99.24%. According to [20], three ML algorithms are tested for their capacity to detect fraudulent charges on credit cards: ANN, RF, and SVM. According to their findings, when it comes to detecting fraudulent transactions, RF outperforms SVM but falls short of ANN.

III. METHODOLOGY

Digital fraud and the damages it causes have skyrocketed alongside the e-commerce industry's meteoric rise. Strong cyber security and anti-fraud measures are essential for establishing a thriving e-commerce sector. Unfortunately, there aren't enough real-world datasets, so research on fraud detection systems has lagged behind. Research and applications in this subject have been rejuvenated by advances in artificial intelligence (AI), Machine Learning (ML), and cloud computing. There have been several assessments that have focused on the use of ML and data mining techniques in e-commerce platforms for the purpose of fraud detection. The complexity of ML algorithms as they pertain to online shopping is beyond the scope of the current evaluations, which only offer high-level descriptions.

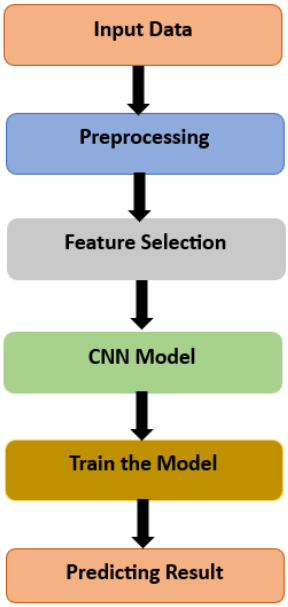

Fig. 1. Threat Cycle of Fraud

A Convolutional Neural Network (CNN) model is used for predictive analysis, as shown in the flow diagram in figure 1. Gathering raw data for processing is the first step in the process, which is called the Input Data. Cleaning, normalizing, and otherwise getting the data ready for analysis is what happens next in the preprocessing stage. To improve the model's efficiency and cut down on computational burden, the Feature Selection step involves identifying key features. Following this, the CNN Model is utilized, and the network is trained to recognize patterns and correlations by means of the Train the Model step. The model's predictions, based on the trained network, are delivered in the Predicting Result phase, which offers practical insights. An organised method for applying CNNs to detection or classification jobs is shown in this process.

A. Preprocessing

1) Dicritization:

Discretization is used for preprocessing and to decrease the intervals of values for attributes. Separation turns the limited set of intervals into continuous features. All intervals have a discrete numerical value. Applying discrete values appropriately improves data mining modeling performance and is highly beneficial for identifying frauds in e-commerce detection systems.

2) Min-max Normalization:

The normalization method breaks down the attribute values. The process of normalization reduces the size of the attributes and simplifies the database. Standardization employs a succession of rules to evaluate the relationship between individuals. The normalization can be expanded to a higher extent according to these guidelines. Following discretization, min-max normalization is carried out. The complete dataset is normalized before testing and training[21]. Data avoidance is ensured by this. The original data undergoes linear modifications in the min-max method. The variables i_{min} and i_{max} reflect the minimum and maximum values in the default of credit card client's dataset. In the min-max algorithm, the mapping from i to i' is provided by

$$i' = \frac{i - i_{min}}{i_{max} - i_{min}}(new\_i_{max} - new\_i_{min}) + new\_i_{min} \quad (1)$$

B. Feature Selection

Data mining and knowledge-based authentication rely on feature selection. In fields like statistics, pattern recognition, and machine learning, where datasets with a high number of features are accessible, the subject of feature selection has been extensively researched. After realizing that most data mining systems spend the vast majority of their resources on cleaning and preparing the data, they came up with a new features selection approach based on Hausdorff distance to analyze online traffic data. Problems with missing information, noisy or irrelevant features, not the best set or mix of features, and other issues might arise from feature selection, which is crucial for every learning process[22]. During the characteristic's selection phase of our investigation, we utilized the simplest statistical technique. A powerful tool for feature selection is the t-statistic. The ranking of the features is done using the formula described below. We propose the t-statistic for use in bioinformatics feature selection.

$$t - statistic = \frac{|\varphi_1 - \varphi_2|}{\sqrt{\frac{\tau_1^2}{r_1} + \frac{\tau_1^2}{r_2}}} \quad (2)$$

τ_1 and τ_2 are the standard deviations of the samples of non-fraudulent firms and fraudulent companies for a given feature, respectively, where φ_1 and φ_2 are the means of the samples of scam companies and legitimate companies for that feature. The supplied feature is represented by the number of samples of non-fraudulent companies r_2 and fraudulent companies r_1. Every feature has its t-statistic calculated; in the first case, the top 18 features with the highest t-statistics are examined, and in the top 10 features.

C. Training the Model

1) CNN:

By calculating a weighted average over nearby words, a simple filter

$$O^{(x)} = \begin{bmatrix} 0.5 & 1 & 0.5 \\ 0.5 & 1 & 0.5 \\ \cdots & \cdots & \cdots \\ 0.5 & 1 & 0.5 \end{bmatrix} \quad (3)$$

making the presentation of trigram units not so unpleasant. Within the context of one-dimensional convolution, every filter matrix $O^{(x)}$is limited to having non-zero values at row x.It follows that $X_s = X_j$and that a distinct filter processes each dimension of the word embedding.

A technique called broad convolution can be used to handle the beginning and end of the input by padding the base matrix $K^{(0)}$with column vectors of zeros at those locations. The output from each layer will be one unit smaller than the input if padding is not added; this is called narrow convolution[23]. In a more general sense, we might use w_x to represent the width of filter $O^{(x)}$ as the filter matrices do not need to have equal filter widths. Multiple layers of convolution can be applied as suggested by the notation $K^{(0)}$, with the result that $K^{(a)}$is the input to $K^{(a+1)}$
$K^{(A)} \in \mathbb{R}^{X_y \times L}$ is obtained as a matrix representation after A convolutional layers. It is important to aggregate overall word locations to get a fixed-length representation if the instances have varied lengths. Operations like max-pooling and average-pooling can do this.

$$y = maxpool\left(K^{(A)}\right) \Rightarrow y_x = max\left(k_{x,1}^{(A)}, k_{x,2}^{(A)}, \ldots, k_{x,l}^{(A)}\right) \quad (4)$$

$$y = maxpool\left(K^{(A)}\right) \Rightarrow y_x = \frac{1}{L}\sum_{l=1}^{L} k_{x,l}^{(A)} \quad (5)$$

y can now function as a feedforward network layer, leading to $\hat{z}$ as a forecast and $m^{(v)}$ as a loss. By recursively learning the classification loss, the parameters $O^{(x)}, p(\Theta)$can be learned, just like in feedforward networks. This necessitates iteratively backpropagating through the max pooling procedure, with its input being a discontinuous function. However, backpropagation solely uses the argmax m since it only requires a local gradient:

$$\frac{\partial y_x}{\partial k_{x,l}^{(A)}} = \begin{cases} 1, & k_{x,l}^{(A)} = max\left(k_{x,1}^{(A)}, k_{x,2}^{(A)}, \ldots, k_{x,l}^{(A)}\right) \\ 0, & otherwise \end{cases} \quad (6)$$

Many of the many convolutional architectures that have been developed for use with image data have found their way into the computer vision literature. Advancements could be made by implementing more intricate pooling algorithms, like k-max pooling, which compiles a matrix containing the k highest values per filter.

IV. Results and Discussion

Problems with security, integrity, and protecting e-commerce products at the time of sale are the most pressing challenges in e-commerce today. Consumers' exaggerated claims about products wind up costing businesses money and disrupting the system as a whole. Using QR code encryption techniques with an alarm system, intrusion detection systems enhance the security of ecommerce systems. An organization's goods can be safeguarded using the proposed system, which encrypts a one-of-a-kind product ID using an image-based method called the QR code system.

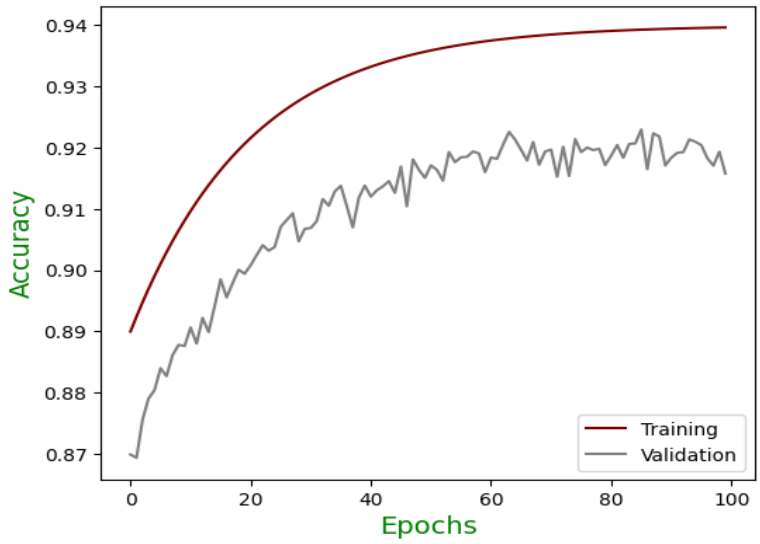

Fig. 2. Training and Validation Accuacy for Fraud Intrusion detection Ecommerce

Figure 2 shows how well an e-commerce fraud and intrusion detection model works. There is a steady improvement in the training accuracy (red line) to over 94% after 100 epochs, and a stabilization of the validation accuracy (gray line) at around 92%. Improving the security of online transactions, such precision is essential for preventing fraud in real time. Advanced approaches, such as CNN-LSTM, have the capacity to detect anomalous activity successfully, as shown by this model.

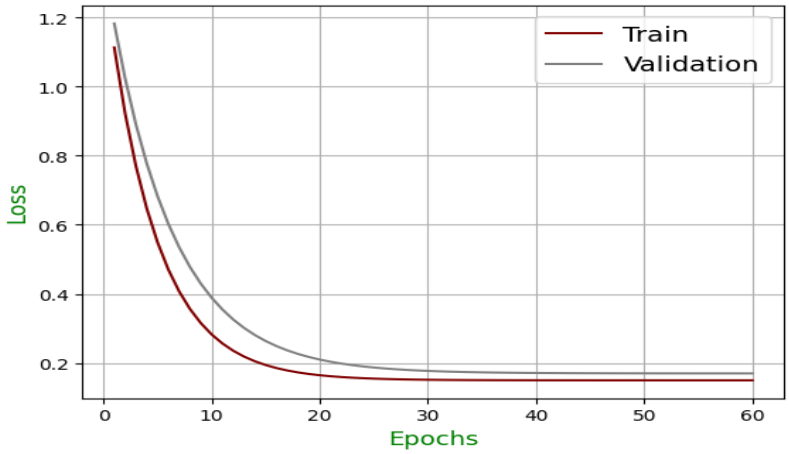

Fig. 3. Training and Validation Accuacy for Fraud Intrusion detection Ecommerce

Figure 3 shows the results of a model for e-commerce fraud and intrusion detection's training and validation losses.

TABLE I. ACCURACY PREDICTION(%)

Metric	**Accuracy**	**Precision**	**Recall**	**Sensitivity**
CNN	95.08	94.40	93.28	97.40
LSTM	91.32	89.54	90.35	95.23
RNN	93.28	91.45	92.38	96.76
XGBoost	89.54	87.39	88.43	94.63

Accuracy, Precision, Recall, and Sensitivity are the four-performance metrics used to compare the various machine learning models (CNN, LSTM, RNN, and XGBoost) in the table. In the context of online store security and fraud prevention, this is how it works. When it comes to e-commerce fraud and intrusion detection, CNN is the best option because it outperforms competitors across the board.

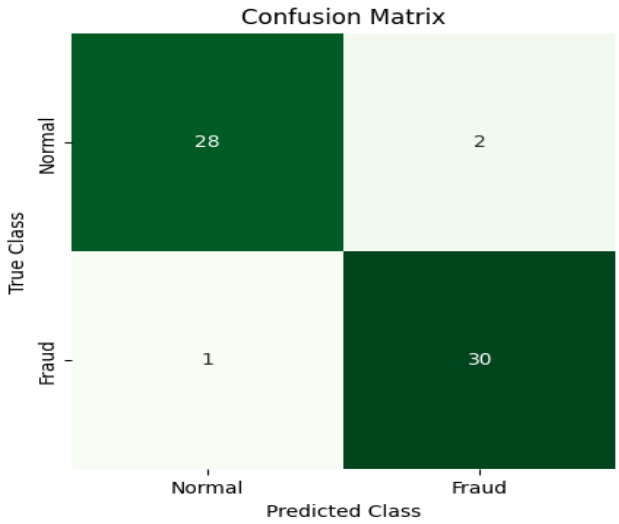

Fig. 4. Confusion Matrix for Fraud Intrusion detection Ecommerce

A fraud detection model's performance in an e-commerce intrusion detection scenario is showcased in Figure 3, which depicts a confusion matrix. The model's capacity to differentiate between regular and fraudulent operations was demonstrated when it successfully recognized 30 fraudulent transactions (True Positives) and 28 genuine transactions (True Negatives). But it missed one fraudulent transaction and incorrectly labelled two valid ones as fraudulent (False Positives and False Negatives, respectively). Based on these findings, the model is highly accurate and reliable, which makes it a promising option for safeguarding e-commerce platforms and detecting anomalies. The methodology strikes a balance between preventing fraud and ensuring client pleasure by minimizing errors.

V. Conclusion and Future Directions

Payment systems for mobile electronic commerce have been developed in response to the requirement for mobile device payments. Detecting two major misuse of electronic payment systems is the focus of this article. Intentional deceit committed with the purpose of obtaining an unfair advantage is known as fraud, and any series of acts designed to undermine the security, privacy, or accessibility of a resource is known as an intrusion. When it comes to electronic payments, the majority of existing fraud and intrusion detection solutions are platform-specific. Since criminal brains quickly adjust their plans and explore new ways to evade existing detection tools, fraud detection is an ever-evolving subject. Furthermore, new criminals join the field, each with their own unique set of skills and mentality. Just because attackers learn about a detection method doesn't imply it's useless.

REFERENCES

[1] D. Massa and R. Valverde, “A Fraud Detection System Based on Anomaly Intrusion Detection Systems for E-Commerce Applications,” *Comput. Inf. Sci.*, vol. 7, no. 2, pp. 117–140, 2014, doi: 10.5539/cis.v7n2p117.

[2] W. Akinola and M. Y. Olumoye, “ANOMALY BASED ONLINE TRANSACTION FRAUD DETECTION SYSTEM ON ANDROID : A SYSTEMATIC REVIEW,” *Res. Gate*, no. December, 2022.

[3] Vikas, R. P. Daund, D. Kumar, P. Charan, R. S. K. Ingilela, and R. Rastogi, “Intrusion Detection in Wireless Sensor Networks using Hybrid Deep Belief Networks and Harris Hawks Optimizer,” in *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, IEEE, Jul. 2023, pp. 1631–1636. doi: 10.1109/ICESC57686.2023.10193270.

[4] P. Akhther, A. Maryposonia, and V. . Prasanth, “Least Square Support Vector Machine based Intrusion Detection System in IoT,” *2023 7th Int. Conf. Intell. Comput. Control Syst.*, pp. 1545–1550, 2023, doi: 10.1109/iciccs56967.2023.10142805.

[5] K. Yamini, V. Anitha, S. Polepaka, R. Chauhan, Y. Varshney, and M. Singh, “An Intelligent Method for Credit Card Fraud Detection using Improved CNN and Extreme Learning Machine,” in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Jun. 2023, pp. 810–815. doi: 10.1109/ICCES57224.2023.10192774.

[6] N. M. Reddy, K. A. Sharada, D. Pilli, R. N. Paranthaman, K. S. Reddy, and A. Chauhan, “CNN-Bidirectional LSTM based Approach for Financial Fraud Detection and Prevention System,” in *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, IEEE, Jun. 2023, pp. 541–546. doi: 10.1109/ICSCSS57650.2023.10169800.

[7] R. Rajkumar, N. Kogila, S. Rajesh, and A. R. Begum, “Intelligent System for Fraud Detection in Online Banking using Improved Particle Swarm Optimization and Support Vector Machine,” in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Jun. 2023, pp. 644–649. doi: 10.1109/ICCES57224.2023.10192690.

[8] A. Sagar, N. K. Anushkannan, G. Indumathi, N. Vasant Muralidhar, D. K A, and P. Malini, “Wireless Sensor Network-based Intrusion Detection Technique using Deep Learning Approach of CNN-GRU,” in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Jun. 2023, pp. 1147–1152. doi: 10.1109/ICCES57224.2023.10192844.

[9] M. A. Jain, B. S. Rao, S. Chattopadhyay, A. Kumar, M. S. Muthuraman, and A. Manjula, “An Artificial Intelligence Network based-Host Intrusion Detection System for Internet of Things Devices,” in *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, IEEE, Jul. 2023, pp. 656–661. doi: 10.1109/ICESC57686.2023.10193232.

[10] K. Rathor, S. Vidya, M. Jeeva, M. Karthivel, S. N. Ghate, and V. Malathy, "Intelligent System for ATM Fraud Detection System using C-LSTM Approach," in *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, IEEE, Jul. 2023, pp. 1439–1444. doi: 10.1109/ICESC57686.2023.10193398.

[11] G. Balakrishna, "A Novel Ensembling of CNN - A - LSTM for IoT Electric Vehicle Charging Stations based on Intrusion Detection System," *2023 Int. Conf. Self Sustain. Artif. Intell. Syst.*, no. Icssas, pp. 1312–1317, 2023, doi: 10.1109/ICSSAS57918.2023.10331735.

[12] S. Kakkar, "Analysis of Discovering Fraud in Master Card based on Bidirectional GRU and CNN based Model," *2023 Int. Conf. Self Sustain. Artif. Intell. Syst.*, no. Icssas, pp. 50–55, 2023, doi: 10.1109/ICSSAS57918.2023.10331770.

[13] M. Jayapal, K. Subhashree, B. Ashwini, D. Satheesh Kumar, S. C. Dimri, and N. Nishant, "Investigation of LSSVM and RBFNN-based Techniques for Intrusion Detection Systems for IoT Networks," *Int. Conf. Self Sustain. Artif. Intell. Syst. ICSSAS 2023 - Proc.*, no. Icssas, pp. 1306–1311, 2023, doi: 10.1109/ICSSAS57918.2023.10331782.

[14] K. Prabhakar, M. S. Giridhar, A. Tatia, T. M. Joshi, S. Pal, and U. S. Aswal, "Comparative Evaluation of Fraud Detection in Online Payments Using CNN-BiGRU-A Approach," *Int. Conf. Self Sustain. Artif. Intell. Syst. ICSSAS 2023 - Proc.*, no. Icssas, pp. 105–110, 2023, doi: 10.1109/ICSSAS57918.2023.10331745.

[15] A. Magadum, A. B. Nadaf, R. Pramodhini, P. Patil, B. Latha, and S. Sivasakthiselvan, "Securing Wireless Sensor Networks: A Novel AlexNet + GRU-Based Intrusion Detection Framework," *2nd Int. Conf. Intell. Data Commun. Technol. Internet Things, IDCIoT 2024*, pp. 1382–1387, 2024, doi: 10.1109/IDCIoT59759.2024.10467623.

[16] T. Porkodi, "An Automatic ATM Card Fraud Detection Using Advanced Security Model Based on AOA-CNN-XGBoost Approach," *2024 Int. Conf. Electron. Comput. Commun. Control Technol.*, pp. 1–7, 2024, doi: 10.1109/ICECCC61767.2024.10593851.

[17] N. Pol and S. Agarwal, "Online Transaction Fraud Detection : Exploring the Hybrid SSA-TCN-BiGRU Approach," *2024 2nd World Conf. Commun. & Comput.*, pp. 1–6, 2024, doi: 10.1109/WCONF61366.2024.10692254.

[18] S. Vii, G. D. Rede, P. Ramesh, R. Kumar A, A. Bharathi, and M. C. J. Anand, "Optimizing E-Commerce Fraud Detection with BiGRU and Capsule Network Architectures," in *2nd IEEE International Conference on Data Science and Network Security, ICDSNS 2024*, 2024, pp. 1–6. doi: 10.1109/ICDSNS62112.2024.10691229.

[19] M. Amini, M., & Rabiei, "Ensemble Learning for Fraud Detection in E-commerce Transactions: A Comparative Study," *J. Appl. Intell. Syst. Inf. Sci.*, vol. 3, no. 2, pp. 65–73, 2022.

[20] A. Mutemi and F. Bacao, "E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review," *Big Data Min. Anal.*, vol. 7, no. 2, pp. 419–444, 2024, doi: 10.26599/BDMA.2023.9020023.

[21] K. Poongodi and D. Kumar, "Support vector machine with information gain based classification for credit card fraud detection system," *Int. Arab J. Inf. Technol.*, vol. 18, no. 2, pp. 199–207, 2021, doi: 10.34028/IAJIT/18/2/8.

[22] P. Ravisankar, V. Ravi, G. Raghava Rao, and I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques," *Decis. Support Syst.*, vol. 50, no. 2, pp. 491–500, 2011, doi: 10.1016/j.dss.2010.11.006.

[23] S. Eisenstein, "Natural Language Processing," in *Give Us Bread but Give Us Roses*, Routledge, 2013, pp. 9–17. doi: 10.4324/9780203103517-5.