Revolutionizing E-Commerce Security: Unveiling an Innovative Deep Learning-Based Strategy for Detecting Financial Fraud

Aditi Sharma [1], S. Phani Praveen[2], Vipin Tiwari[1], Pradeep Kumar Arya[3,*], Deepak Parvathaneni Naga Srinivasu[4], Mukta Patel[5]

[1]Department of Computer Science and Engineering, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, India

[2]Department of CSE, PVP Siddhartha Institute of Technology, Vijayawada, A.P, India

[3]School of Computer Science Engineering and Technology, Bennett University, Grater Noida, UP, 201310, India

[4]Department of CSE, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Amaravati 522503, Andhra Pradesh, India

[5]Department of CSE, Parul Institute of Technology, Parul University, Vadodara, Gujarat, India

Emails: aditi.sharma@ieee.org; sppraveen@pvpsiddhartha.ac.in; vipintiwari1@gmail.com; pradeeparya25@gmail.com; p_nagasrinivasu@av.amrita.edu; muktapatel0285@gmail.com

Abstract

An inventive deep learning-based method for identifying financial fraud, revolutionizing e-commerce security in the process. The research offers a state-of-the-art setup that makes use of deep learning computations in the dynamic world of online exchanges, where the possibility of fraudulent activity is a danger. Since frauds are known to be erratic and lack consistency, it might be challenging to spot them. Con artists exploit the latest developments in technology. They manage to evade security measures, which results in millions of dollars being lost. One method of tracking fraudulent exchanges is to use information-mining techniques to investigate and detect unusual behaviours. Interactions. In contrast to deep learning techniques as auto encoders, convolutional neural networks (CNN), restricted Boltzmann machines (RBM), and deep belief networks (DBN), this paper aims to benchmark several machine-learning techniques, such as k-nearest neighbour (KNN), irregular forest, and support vector machines (SVM). The three-evaluation metrics that are really employed are the Area Under the ROC Curve (AUC), the Matthews Correlation Coefficient (MCC), and the Cost of Failure.

Keywords: Novel Approach; Financial; Fraud Detection; Deep Learning; E-Commerce; Machine Learning

1. Introduction

Unquestionably, the rapid growth of e-commerce has changed the way we conduct business and conduct trades. While it provides unmatched convenience, it also presents an increasingly complicated terrain of security risks. Financial fraud is becoming a more serious threat to the computerized economy, thus new and creative ways to protect online transactions are required. This research explores the field of e-commerce security revolution and presents a novel method that reveals a deep learning-based strategy specifically intended for financial fraud detection.

Financial fraud in the e-commerce industry has advanced in sophistication in recent years, taking advantage of weaknesses in traditional security procedures. Conventional techniques, such as signature-based detection and rule-based systems, have demonstrated their limitations in keeping up with the ever-evolving tactics used by cybercriminals [1]. The suggested approach makes use of deep learning, a portion of artificial intelligence, to offer a flexible and clever defense system. Deep learning computations, which draw inspiration from the neural

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

networks found in the human brain, demonstrate an amazing ability to recognize intricate patterns and make judgments based on vast amounts of data.

The integration of deep learning algorithms to analyze contextual data, user behavior, and value-based information in real-time is the main emphasis of this research. As a result, it aims to improve fraud detection's accuracy and effectiveness by spotting unusual patterns that could indicate fraudulent activity. The adaptability of the suggested approach is what makes it novel; it not only tackles existing fraud tactics but also changes to meet new threats, guaranteeing a proactive defense that keeps up with the rapidly evolving cyber environment.

The importance of this technique becomes clearer as we continue our investigation on a deep learning-based method for identifying financial crime in e-commerce. This research has the potential to have an impact that goes beyond improving security alone. It might boost user confidence in the sophisticated marketplace and reinforce the foundation of trust that supports the thriving e-commerce industry.

2. Literature Survey

Ashtiani and Raahemi (2021) provide a thorough investigation of the use of information mining and machine learning approaches for intelligent fraud detection in financial accounts [2]. Their comprehensive evaluation of the literature, which was published in IEEE Access, essentially assesses the range of previous studies in this field. The paper explores several machine learning computations and information mining techniques used on financial datasets in order to more precisely detect fraudulent activity. The authors stress how crucial it is to use complex computations to combat the changing face of financial crime. Key trends and issues in the industry are identified by the review, including the requirement for creative approaches to combat more complex fraudulent schemes. The amalgamation of research findings in this study is a beneficial tool for scholars, professionals, and decision-makers that aim to improve fraud detection systems within the financial industry.

Chaquet-ulldemolins, Moral-rubio, and Muñoz-romero (2022) add to the body of knowledge on fraud detection by tackling the black-box problem with interpretable auto encoders and nonlinear analysis [3]. Published in Applied Sciences, their review delves into the complexities of fraud detection models that frequently lack interpretability. The authors intend to use auto encoders in order to improve these models' transparency while maintaining their capacity to identify intricate, nonlinear patterns that are suggestive of fraudulent activity. The study emphasizes how important interpretable artificial intelligence models are for fundamental tasks like fraud detection, where comprehension of the decision-making process is essential. The review provides insightful insights into the trade-off between interpretability and model complexity, illuminating how auto encoders could be used to effectively fill this gap.

Da'U and Salim (2019) provide a systematic overview and new directions in the field of recommendation systems based on deep learning techniques [4]. Their paper, which was published in the Man-made Consciousness Review, examines how recommendation systems have changed over time, highlighting the revolutionary potential of deep learning techniques. Deep neural networks and neural collaborative filtering are only two examples of the many deep learning approaches used in recommendation systems that are covered in this article. To set up future research paths, the developers essentially evaluate the advantages and disadvantages of current methods. Because of its thoroughness, this review is a vital tool for practitioners and researchers who want to use deep learning to create effective and personalized recommendation systems.

In the area of financial fraud, Hilal, Gadsden, and Yawney (2021) lead an extensive review of peculiarity detection strategies [5]. The review, which was published in Expert Systems Applications, offers insights into how strangeness detection techniques have advanced and how the field of financial fraud detection is changing. The authors examine various methodologies, ranging from conventional factual methods to contemporary machine learning computations, with the aim of detecting irregularities suggestive of deceitful actions in monetary transactions. In order to improve the resilience of irregularity detection systems in the financial sector, researchers, practitioners, and policymakers can benefit greatly from the review, which summarizes current research trends, obstacles, and recent advancements in the field of financial fraud detection.

In Engineering Applications, Isong and Bekele (2013) provide a comprehensive analysis of mobile agents' ability to adapt to non-critical failures. The paper examines the methods and strategies for guaranteeing non-critical failure adaption in mobile agent systems, where agents move independently between hosts to carry out tasks [6]. The authors essentially review the literature that has already been written on the subject of mobile agent environments, covering topics like system resilience, recovery mechanisms, and deficiency detection. Researchers and practitioners involved in the design and implementation of fault tolerant mobile agent systems will find this systematic review to be a useful resource as it provides insights into state-of-the-art approaches and identifies areas that warrant additional investigation.

Marcotte and Petrillo (2019) conducted a thorough assessment of different adaptation to non-critical failure mechanisms, which advances our understanding of adaptation to internal failure in cloud systems [7]. The paper,

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

which was presented at the IEEE International Conference on Software Reliability Engineering Workshops (ISSREW), examines several strategies used in distributed computing settings to adapt to non-critical failure mechanisms. The authors, providing insight into how well they work to guarantee the dependability and durability of cloud-based services, analyze the mechanisms' strengths and weaknesses. This systematic study provides a thorough overview of numerous adaptations to non-critical failure mechanisms, which is helpful in guiding academics and practitioners in the field of distributed computing and preparing the way for the development of robust and powerful cloud systems.

A. Current Challenges in E-Commerce Security

In the modern digital world, e-commerce security faces several obstacles that call for a flexible and all-encompassing strategy to protect financial transactions. The constant evolution of cyber threats, where hackers are using more advanced techniques to target weaknesses in e-commerce stages, is one major cause for concern [8][9]. To keep ahead of obnoxious entertainers, creative solutions are needed to address the ongoing threat of unauthorized access, information breaches, and financial theft.

Furthermore, the difficulty of promptly and accurately detecting fraudulent actions is exacerbated by the sheer volume and complexity of exchanges inside the e-commerce ecosystem. Conventional security solutions, which frequently depend on rule-based systems, find it difficult to keep up with the evolving and complex nature of new threats. This emphasizes the need for new tactics that make use of cutting-edge technology to identify minute patterns that could be signs of fraud in order to maintain the security of online financial transactions [10][11].

A thorough and innovative strategy to security is required due to the diverse nature of the issues posed by the expanding and diversifying e-commerce sectors [12]. The adoption of cutting-edge technologies, such as deep learning-based tactics, appears to be a viable way to manage the changing threat landscape and create a safe foundation for e-commerce in the future.

B. Deep Learning as a Revolutionary Approach

In spite in the field of e-commerce security, deep learning is unique as a breakthrough method that has altered our perspective on the difficult problems involved in protecting financial transactions. Fundamentally, deep learning is a branch of machine learning that uses artificial neural networks that can recognize complex patterns and representations from data. Deep learning models, in contrast to traditional rule-based systems, are highly proficient in identifying intricate and non-linear associations, which makes them highly suitable for the ever-changing and dynamic realm of cyber threats inside the e-commerce industry [13].

Deep learning's ability to automatically extract hierarchical features from unprocessed data is one of its main advantages since it enables the technology to recognize minute patterns that may be signs of fraud. This is particularly critical in the context of e-commerce, where sophisticated fraud methods are constantly evolving. Similar to neural networks, deep learning algorithms can adapt to and learn from enormous amounts of data, allowing them to find abnormalities and hidden links that would defy traditional security procedures.

Deep learning models are also well suited for real-time processing due to their flexibility, which is a fundamental need in the fast-paced world of online exchanges. Real-time information stream analysis improves security systems' responsiveness by facilitating the prompt identification and mitigation of possible threats [14,15]. This flexibility in real-time is especially important considering how quickly cyber-attacks may spread throughout the e-commerce industry.

Deep learning [16],[17] is a novel approach that provides superior irregularity detection skills and opens the door for continuous development. These algorithms are able to adapt to new risks and changing trends in fraudulent activity since they may be trained on dynamic datasets. Deep learning systems are unique and future-verification tools for e-commerce security because of their self-learning capabilities, which provide a strong defense against the dynamic array of cyber threats in the digital marketplace.

C. Unveiling the Innovative Deep Learning-Based Strategy

In terms of e-commerce security, revealing the cutting-edge deep learning-based approach represents a significant advancement in fortifying financial transactions against dynamic cyber threats [18]. Fundamentally, this approach makes use of the power of sophisticated deep learning computations, particularly neural networks, to examine and decipher intricate patterns inside enormous datasets. The novel part is how these deep learning methods are incorporated into a unified, flexible framework created especially to identify and stop financial crime.

The first step in the technique is to create a strong, dynamic model that has been trained on a variety of datasets that contain verifiable conditional data. By identifying common user behaviour patterns, the deep learning model creates a baseline against which anomalies suggestive of possibly fraudulent activity can be detected. Deep

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

learning's adaptability enables the model to continuously adapt to and learn from new data, keeping it aware of new threats and changing tactics used by hackers [19].

Moreover, the plan integrates real-time information streams to provide prompt inquiry and reaction to ongoing conversations. The capacity to process data in real-time is crucial in the fast-paced and high-volume e-commerce industry, since it enables prompt and precise detection of fraudulent activity. In this way, the deep learning-based method guarantees a proactive approach to security, minimising the possible impact of fraud on both companies and customers.

Investigating block chain technology is a crucial part of the creative plan. The plan aims to improve exchange integrity and traceability by incorporating the block chain's immutability and transparency. This solves issues of accountability and fraud prevention in addition to providing an additional degree of protection. The distributed and networked structure of e-commerce stages is perfectly suited to the decentralised nature of block chain technology.

To put it simply, revealing this cutting-edge deep learning technique provides a complete and flexible approach to e-commerce security [20][21]. The method offers a comprehensive defence against financial fraud by combining the power of deep learning calculations, real-time information processing, and block chain technology. It also sets a new standard for security measures in the dynamic and linked world of online exchanges [22].

3. Proposed Methodology

The performance of divergent classification techniques is evaluated under divergent experimental setup to analyze the performance of each of those classification techniques under distinct experimental setups. Initially, the dataset is split as 70-30, i.e., 70% is used for training the model and 30% is used for validating the model, considered as Setup-1. In the subsequent phase, the model is evaluated at 80-20 split, i.e., 80% is used for training the model and 20% is used for validating the model, considered as Setup-2. Finally, the model is evaluated at 90-10 split, i.e., 70% is used for training the model and 30% is used for validating the model, considered as Setup-3.

3.1 Dataset Description

The Three distinct types of data will be used in this study's studies. The Indian Dataset contains the trades made by credit card users over a two-day period in September 2020. With the exception of time and amount, PCA changes have been made to every field. Just 492 occurrences—or 216,809 incidents overall—involve fraud. We utilized the UCI ML repository to obtain the Indian Dataset. To ensure that no personally identifiable information was revealed, the data's sources were kept under wraps.

There are 300 incidences of fraud compared to 324 cases of normal behavior. In the meantime, out of the 1100 samples in the other informational collection, 350 are attempts at fraud and the other 600 are real. India's data is considered.

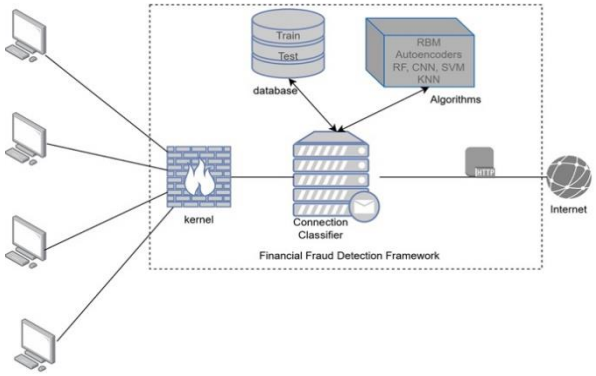

Figure 1. Block Diagram of the Proposed Classification Model.

3.2 Measures of Performance

We go into detail about the key elements to consider while evaluating this concentration in the sections that follow. A metric called the Matthews connection coefficient is employed to measure the manifestation of an equal or two-class classifier. Psyche W. Matthews first put forth this idea in 1975. A coefficient value of one indicates an accurate gauge, whereas a value of zero indicates an unreliable gauge. The phi coefficient can also be thought of

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

as the Matthews connection. According to Davide Chicco, exactness and F1 score have some limitations, while MCC considers all four net rescue values, making it the most reliable measure.
The beneficiary's presentation is addressed by the ROC bent. The inconsistent concept of the data gathering allows for the accuracy of the model to be assessed. The TPR on centre x and the FPR on centre y are the sole figures that the ROC bend depicts. When the two ROC bends' regions under the curve (AUC) are similar, more details, including disappointment costs, ought to be investigated. The following formula is used to calculate harm charges: $1,000 for each false positive (a deception that is documented true to form) and $100 for each false negative (a typical extortion case that is considered a misrepresentation). Because MCC and AUC values were often broadly equal, we used this system to analyse the three main models. The cost of the next troupe classifiers is also established in the same way.

4. Results and Discussion

The results of the tests conducted on the Indian Dataset are now provided. The ensemble of the approaches KNN, SVM, and CNN is considered as Ensemble 1 and the ensemble of the approaches KNN, SVM, RF is assumed as Ensemble 2. The confusion matrix obtained on experimentation is shown in Figure 2.

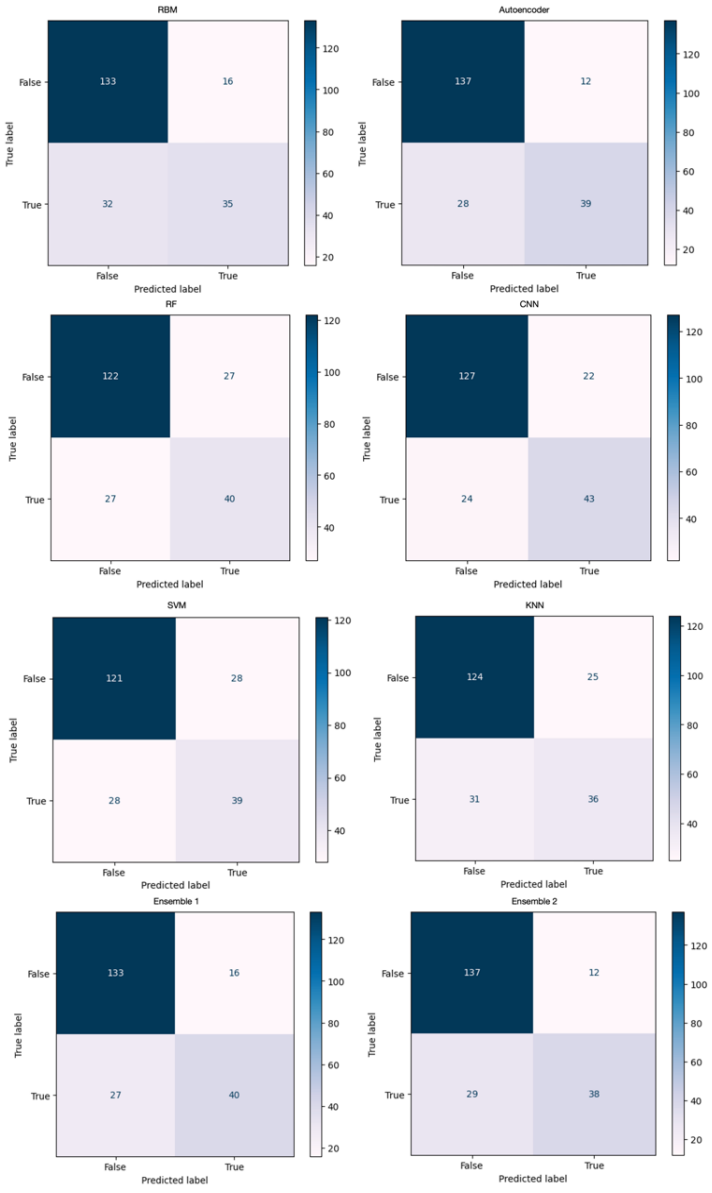

Figure 2. Confusion matrix of various classification models under setup-1.

4.1. Experimental outcome in Setup-1

The experimental results of setup-1 of the dataset are shown in Table-1 and the corresponding figures are shown in Fig 3, 4 and 5.

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

Table 1: Performance Outcome under Experimental Setup-1

Method	***MCC***	***AUC***	***Accuracy***	***F1-Score***
RBM	0.175	0.899	0.777	0.847
Auto encoders	0.256	0.892	0.815	0.872
RF	0.792	0.818	0.750	0.818
CNN	0.829	0.854	0.787	0.864
SVM	0.825	0.902	0.740	0.812
KNN	0.825	0.882	0.740	0.815
Ensemble 1	0.823	0.891	0.800	0.860
Ensemble 2	0.842	0.901	0.810	0.869

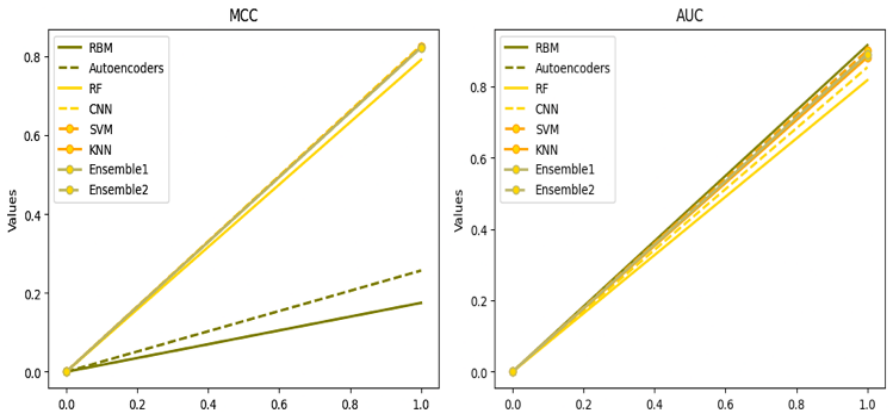

Figure 3. Graphs representing the MCC and AUC performance under experimental setup-1.

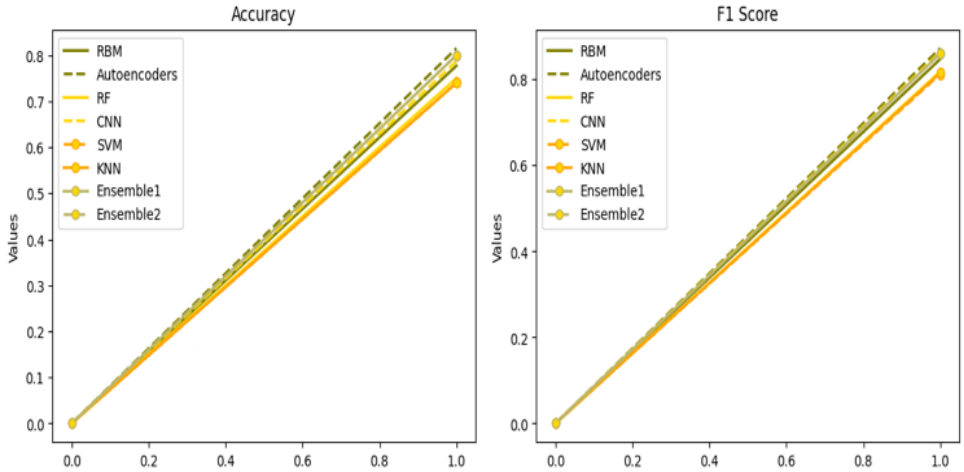

Figure 4. Graphs representing the accuracy and f1-score performance under experimental setup-1.

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

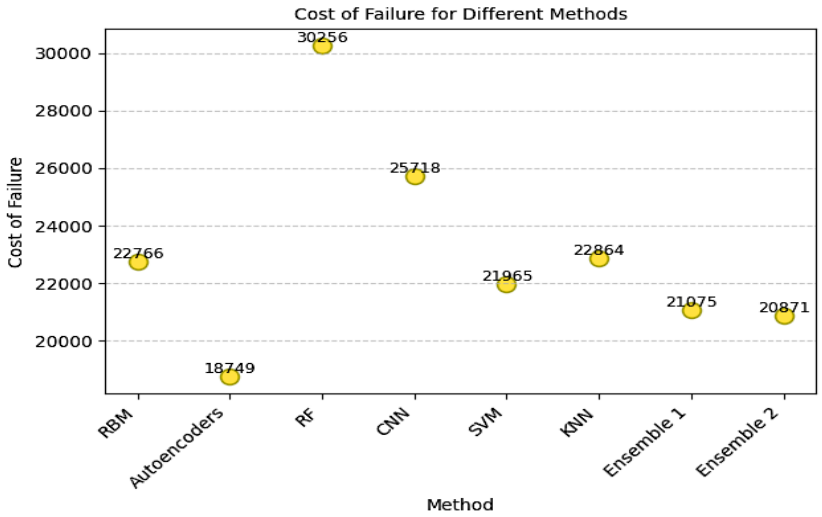

Figure 5. Graph of cost to failure for dataset results for first partition

A brief summary of the findings from the Indian dataset is provided in Table I. RBM and AE perform poorly in terms of MCC and cost because of their high false positive rates (also known as false caution rates). For Arbitrary Forest, the MCC and AUC are both acceptable. The highest MCC and AUC are attained by CNN, SVM, and KNN. It is evident that SVM has a far lower cost of failure than RBM and auto encoders do. Arbitrary forest works well, but it costs a lot of money.

The three best-performing models are combined to create the bigger component voting classifier. Even though the ensemble approach costs about the same as SVM, it performs better than SVM or CNN by itself. On the other hand, SVM has a higher AUC. In this case, the ensemble approach would take more time to prepare for and run tests on, whereas SVM uses the least energy. It is advised to employ SVM rather than the ensemble if the organization intends to cut costs as much as is reasonably possible.

4.2. Experimental outcome in Setup-2

The experimental results of setup-1 of the dataset is shown in Table 2 and the corresponding figures are shown in Fig 6,7 and 8.

Table 2: Performance Outcome under Experimental Setup-2

Method	***MCC***	***AUC***	***Accuracy***	***F1-Score***
RBM	0.1567	0.5285	0.812	0.861
Autoencoders	0.2363	0.6150	0.839	0.893
RF	0.6256	0.8256	0.792	0.834
CNN	0.616	0.8267	0.822	0.887
SVM	0.6918	0.8440	0.772	0.830
KNN	0.7028	0.8927	0.759	0.847
Ensemble 1	0.7250	0.8257	0.896	0.899
Ensemble 2	0.7253	0.8259	0.902	0.932

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

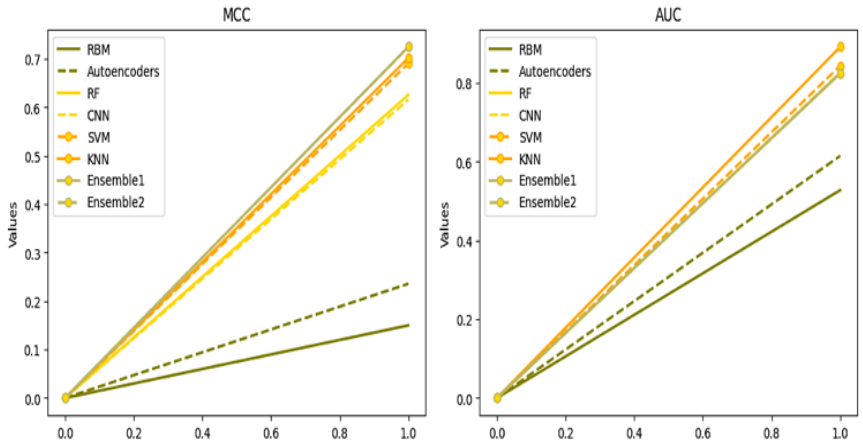

Figure 6. Graphs representing the MCC and AUC performance under experimental setup-2.

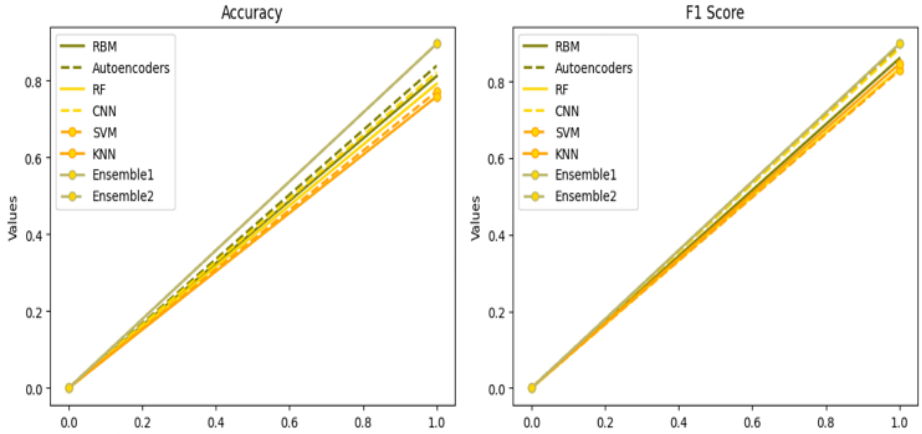

Figure 7. Graphs representing the accuracy and f1-score performance under experimental setup-2.

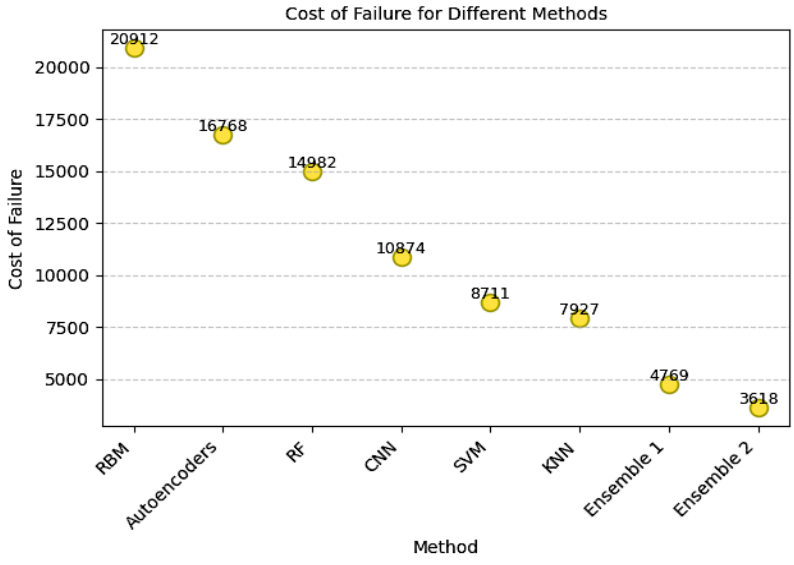

Figure 8. Graph of cost to failure for dataset results for experimental setup-2.

The results of the other dataset are summarized in Table II. Naturally, out of all the methods that are currently in use, RBM and AE produce the worst results. The best AUC and MCC are exhibited by SVM, DBN, and KNN. CNN and Strange Backwoods are big projects in the interim. Our focus is on these two global models. The three classifiers in the primary gathering model (Set 1) are KNN, DBN, and SVM. The models with the lowest disappointment costs, KNN, SVM, and Sporadic Woods, are used to put together the next set (set 2). Due to the vast number of deceptive benefits caused by the edge, RBM and AE have the highest disappointment costs.

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

Table-2 shows that Set 1 (KNN, SVM, and DBN) outperforms independent SVM and other techniques in terms of MCC and AUC. Still, the cost is more than that of irregular forests and help vector machines. One possible explanation is the high error esteem costs associated with KNN and DBN. Set 2 (KNN, SVM, Inconsistent Backwoods) connects the classifiers with the least amount of damaged processes to produce classifiers with higher MCC, AUC, and cost values. In this case, we discovered that the combined methods generally produced better outcomes, with Set 2 turning out to be the better choice due to its reduced cost and higher MCC and AUC values.

4.3 Experimental outcome in Setup-3

Table 3: Response to Dataset

Method	***MCC***	***AUC***	***Accuracy***	***F1-Score***
RBM	0.098	0.551	0.803	0.857
Auto encoders	0.140	0.518	0.829	0.881
RF	0.248	0.690	0.788	0.829
CNN	0.279	0.528	0.816	0.877
SVM	0.209	0.629	0.769	0.828
KNN	0.401	0.701	0.750	0.846
Ensemble 1	0.442	0.729	0.891	0.889
Ensemble 2	0.457	0.734	0.899	0.924
Ensemble 2	0.457	0.734	0.899	0.924

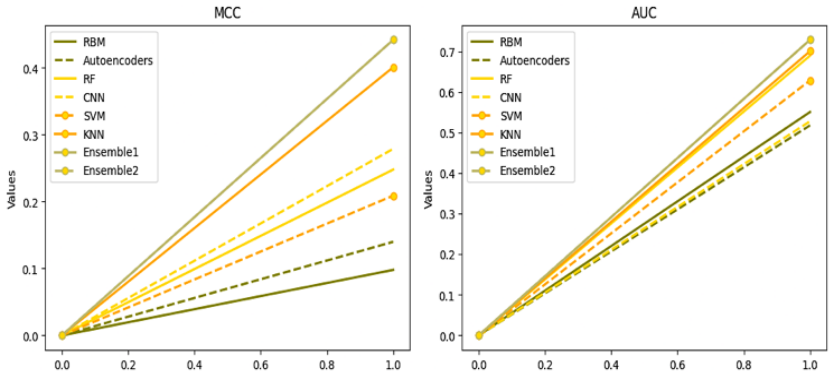

Figure 9. Visual Representation of Dataset Response.

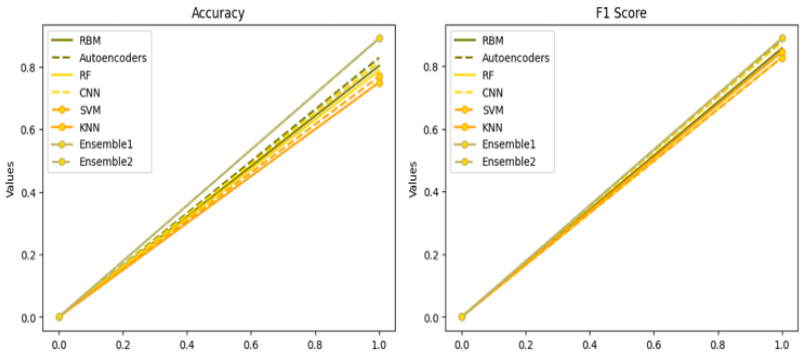

Figure 10. Graphs representing the accuracy and f1-score performance under experimental setup-3.

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

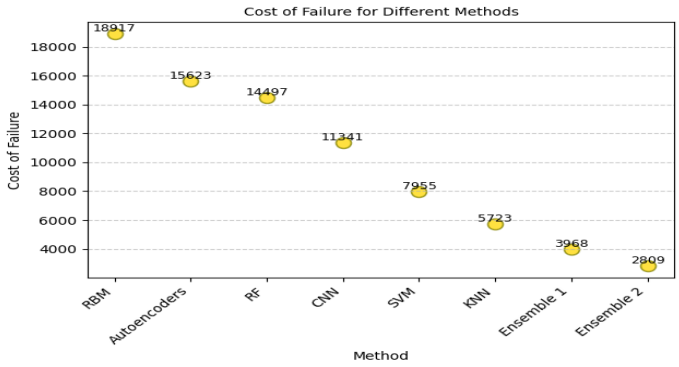

Figure 11. Graph of cost to failure for experimental setup-3.

Table- 3 summarizes the results for the Other Dataset. The most efficient models are CNN, SVM, and Irregular Forest, based on the data in the table. Additionally, compared to other models, the failure cost of models like CNN, SVM, and irregular forest is cheaper. Consequently, we use an ensemble of these three models to create most of the voting-based classifier. The RoC curves obtained on experimentation of the model with experimental settings of setup 1 is shown in Figure 3.

For the three data sets that were tested, the results presented in Tables 1, 2, and 3 demonstrate that it is more prudent to integrate the best models rather than using individual models. When estimating extra point-by-point information, the overall improvement is more apparent. It produces results for the Indian dataset that are a little less accurate than SVM. Irregular Forest works well with smaller datasets. Convolutional neural networks, which rank fourth on the II dataset and perform well on both the Indian and I datasets while having an expenditure of failure similar to KNN, were shown to be the best deep learning technique. It also had the dataset's lowest expense.

5. Conclusion

The discovery of a novel deep learning-based method for identifying financial fraud has marked a significant milestone in the effort to transform e-commerce security. This solution, which makes use of deep learning techniques, demonstrates how e-commerce stages are approaching security concerns from a different angle. With neural network complexities, the suggested method exhibits an enhanced ability to identify subtle patterns and irregularities inside financial transactions, hence enhancing the defences against fraudulent operations. In addition to improving fraud detection's accuracy and efficiency, the combination of cutting-edge deep learning techniques handles the dynamic nature of cyberthreats in the robust e-commerce market. This innovative approach promises to rewrite the rules for securing financial transactions in the digital sphere, making it a pivotal point in strengthening the security framework of online exchanges.

With its novel approach to financial fraud detection based on deep learning, e-commerce security has a bright future ahead of it. Constant improvements in deep learning computations, along with the possibility of incorporating technologies like edge processing and block chain, should improve and enhance the accuracy and adaptability of the approach. Staying ahead of new dangers will require ongoing research efforts and collaboration among industry stakeholders. This deep learning arrangement's adaptability and accessibility will be crucial, guaranteeing its broad adoption and establishing new standards for security guidelines in the e-commerce industry. In the end, the idealized future comprises a dependable and safe electronic commerce environment that successfully combats financial crime by utilizing innovative technologies.

References

[1.] Al-Hashedi, K.G.; Magalingam, P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Comput. Sci. Rev. 2021, 40, 100402.
[2.] Ashtiani, M.N.; Raahemi, B. Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review. IEEE Access 2021, 10, 72504–72525.
[3.] Chaquet-ulldemolins, J.; Moral-rubio, S.; Muñoz-romero, S. On the Black-Box Challenge for Fraud Detection Using Machine Learning (II): Nonlinear Analysis through Interpretable Autoencoders. Appl. Sci. 2022, 12, 3856.
[4.] Da'U, A.; Salim, N. Recommendation system based on deep learning methods: A systematic review and new directions. Artif. Intell. Rev. 2019, 53, 2709–2748.
[5.] Hilal, W.; Gadsden, S.A.; Yawney, J. Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. Expert Syst. Appl. 2021, 193, 116429.
[6.] Isong, B.E.; Bekele, E. A systematic review of fault tolerance in mobile agents. Eng. Appl. 2013, 2, 111–124.

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024

[7.] Marcotte, P.; Petrillo, F. Multiple Fault-tolerance Mechanisms in Cloud Systems: A Systematic Review. In Proceedings of the 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Berlin, Germany, 28–31 October 2019; pp. 414–421.
[8.] Choi, D.; Lee, K. An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation. Secur. Commun. Netw. 2018, 2018, 1–15.
[9.] Naga Srinivasu, Parvathaneni, et al. "Probabilistic Buckshot-Driven Cluster Head Identification and Accumulative Data Encryption in WSN." Journal of Circuits, Systems and Computers 31.17 (2022): 2250303.
[10.] Mohammadian, V.; Navimipour, N.J.; Hosseinzadeh, M.; Darwesh, A. Comprehensive and systematic study on the fault tolerance architectures in cloud computing. J. Circuits Syst. Comput. 2020, 29, 2050240
[11.] Nassif, A.B.; Abu Talib, M.; Nasir, Q.; Dakalbab, F.M. Machine Learning for Anomaly Detection: A Systematic Review. IEEE Access 2021, 9, 78658–78700.
[12.] S. P. Praveen, S. Sindhura, P. N. Srinivasu and S. Ahmed, "Combining CNNs and Bi-LSTMs for Enhanced Network Intrusion Detection: A Deep Learning Approach," 2023 3rd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2023, pp. 261-268, doi: 10.1109/ICCIT58132.2023.10273871.
[13.] Patil, S.; Nemade, V.; Soni, P. ScienceDirect Predictive Modelling for Credit Card Fraud Detection Using Data Analytics. Procedia Comput. Sci. 2018, 132, 385–395.
[14.] Randhawa, K.; Loo, C.K.; Seera, M.; Lim, C.P.; Nandi, A.K. Credit Card Fraud Detection Using AdaBoost and Majority Voting. IEEE Access 2018, 6, 14277–14284.
[15.]Arava, Karuna, et al. "Sentiment Analysis using deep learning for use in recommendation systems of various public media applications." 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2022.
[16.] V. Vankadaru, P. N. Srinivasu, S. H. H. Prasad, P. Rohit, P. R. Babu and M. D. C. Raju, "Text Identification from Handwritten Data using Bi-LSTM and CNN with FastAI," 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 2023, pp. 215-220, doi: 10.1109/ICIDCA56705.2023.10099715.
[17.] Praveen, S. P., Chokka, A., Sarala, P., Nakka, R., Chandolu, S. B., & Jyothi, V. E. (2024). Investigating the Efficacy of Deep Reinforcement Learning Models in Detecting and Mitigating Cyber-attacks: a Novel Approach. Journal of Cybersecurity & Information Management, 14(1).
[18.] Ryman-Tubb, N.F.; Krause, P.; Garn, W. How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. Eng. Appl. Artificial. Intelligence. 2018, 76, 130–157.
[19.] West, J.; Bhattacharya, M. Intelligent financial fraud detection: A comprehensive review. Computer. Secure. 2016, 57, 47–66.
[20.] Zeng, Y.; Tang, J. RLC-GNN: An Improved Deep Architecture for Spatial-Based Graph Neural Network with Application to Fraud Detection. Appl. Sci. 2021, 11, 5656.
[21.] Praveen, S. Phani, et al. "A robust framework for handling health care information based on machine learning and big data engineering techniques." International Journal of Healthcare Management (2022): 1-18.
[22.]Praveen, S. P., Bikku, T., Muthukumar, P., Sandeep, K., Sekhar, J. C., & Pratap, V. K. (2024). Enhanced Intrusion Detection Using Stacked FT-Transformer Architecture. Journal of Cybersecurity & Information Management, 13(2).

DOI: https://doi.org/10.54216/FPA.170227
Received: February 20, 2024 Revised: May 21, 2024 Accepted: October 24, 2024