IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

CREDIT CARD FRAUD DETECTION USING STATE-OF-THE-ART MACHINE LEARNING AND DEEP LEARNING ALGORITHMS

Mr. S. K. Alisha, Associate professor,
Department of MCA
Khadar6@gmail.com
B V Raju College, Bhimavaram

Bobbadi Akhil (2285351014)
Department of MCA
bobbadiakhil72@gmail.com
B V Raju College, Bhimavaram

ABSTRACT

People can use credit cards for online transactions as it provides an efficient and easy-to-use facility. With the increase in usage of credit cards, the capacity of credit card misuse has also enhanced. Credit card frauds cause significant financial losses for both credit card holders and financial companies. In this research study, the main aim is to detect such frauds, including the accessibility of public data, high-class imbalance data, the changes in fraud nature, and high rates of false alarm. The relevant literature presents many machines learning based approaches for credit card detection, such as Extreme Learning Method, Decision Tree, Random Forest, Support Vector Machine, Logistic Regression and XG Boost. However, due to low accuracy, there is still a need to apply state of the art deep learning algorithms to reduce fraud losses. The main focus has been to apply the recent development of deep learning algorithms for this purpose. Comparative analysis of both machine learning and deep learning algorithms was performed to find efficient outcomes. The detailed empirical analysis is carried out using the European card benchmark dataset for fraud detection. A machine learning algorithm was first applied to the dataset, which improved the accuracy of detection of the frauds to some extent. Later, three architectures based on a convolutional neural network are applied to improve fraud detection performance. Further addition of layers further increased the accuracy of detection. A comprehensive empirical analysis has been carried out by applying variations in the number of hidden layers, epochs and applying the latest models. The evaluation of research work shows the improved results achieved, such as accuracy, f1-score, precision and AUC Curves having optimized values of 99.9%,85.71%,93%, and 98%, respectively. The proposed model outperforms the state-of-the-art machine learning and deep learning algorithms for credit card detection problems. In addition, we have performed experiments by balancing the data and applying deep learning algorithms to minimize the false negative rate. The proposed approaches can be implemented effectively for the real-world detection of credit card fraud.

Keywords: Credit Card Fraud Detection, Machine Learning, Deep Learning, Convolutional Neural Network, Fraud Prevention, Financial Security, Data Imbalance.

INTRODUCTION

Credit card transactions have become an integral part of modern-day financial activities, providing a convenient and efficient means for consumers to conduct online and offline transactions. The widespread use of credit cards has, however, given rise to significant concerns about fraud. Credit card fraud is a major issue that leads to substantial financial losses for both individuals and financial institutions. As the volume of credit card transactions increases, so does the complexity and sophistication of fraudulent activities, necessitating the development of advanced detection systems to safeguard against such threats. The traditional methods of fraud detection have been largely rule-based and dependent on human oversight, which are insufficient in the face of evolving fraud tactics. Machine learning (ML) algorithms have emerged as a powerful tool in detecting fraudulent transactions due to their ability to learn from historical data and identify patterns indicative of fraud. However, while these methods have improved detection rates, they still suffer from limitations such as handling high-class imbalance, adapting to changes in fraud patterns, and minimizing false alarms.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 12, Issue 2, 2024

Recent advancements in deep learning (DL) have shown promise in addressing these challenges by leveraging sophisticated neural network architectures capable of learning complex representations from data. Deep learning models, particularly convolutional neural networks (CNNs), have demonstrated remarkable performance in various domains, including image recognition and natural language processing, and are now being explored for their potential in fraud detection. In this research, we aim to enhance credit card fraud detection by applying state-of-the-art machine learning and deep learning algorithms. We utilize the European card benchmark dataset to conduct a comprehensive empirical analysis and compare the performance of traditional ML algorithms with advanced DL models. The goal is to improve detection accuracy, reduce false positives and false negatives, and provide a robust solution that can be effectively implemented in real-world scenarios.

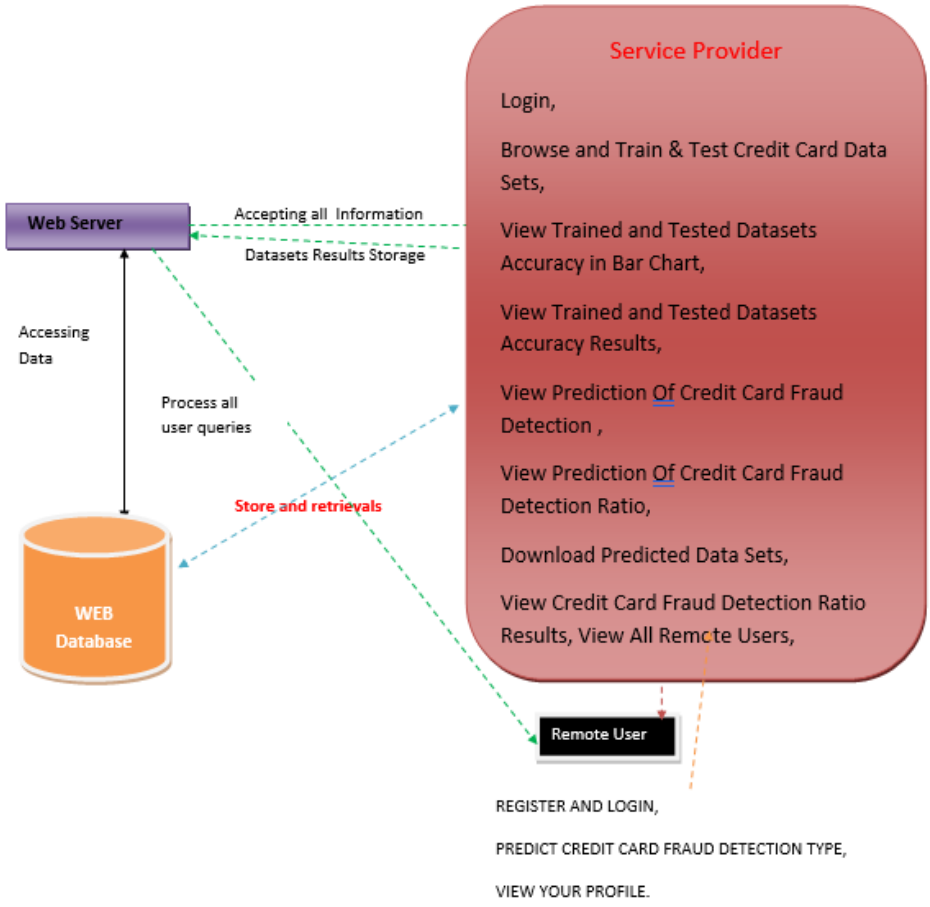

Fig 1: System Architecture

Our study is structured to first apply traditional machine learning algorithms to establish a baseline performance. We then explore the use of deep learning architectures, including variations in the number of hidden layers and epochs, to optimize the detection performance. The results of our experiments demonstrate significant improvements in accuracy, precision, recall, and AUC (Area Under the Curve) metrics, showcasing the superiority of deep learning models in detecting credit card fraud.

LITERATURE SURVEY

ISSN 2347–3657

Volume 12, Issue 2, 2024

Credit card fraud detection has been a topic of extensive research, with numerous studies exploring various machine learning techniques to tackle the issue. Traditional methods, such as rule-based systems, have been widely used but are limited by their inability to adapt to new and evolving fraud patterns. The advent of machine learning has provided new avenues for developing more robust and adaptive fraud detection systems. One of the earliest approaches to fraud detection involved the use of logistic regression and decision trees. Logistic regression, while simple and interpretable, often falls short in capturing the complexities of fraudulent behavior. Decision trees, on the other hand, can handle non-linear relationships but are prone to overfitting, especially in the presence of noisy data.

Random forests, an ensemble learning method, have been shown to improve upon decision trees by aggregating the predictions of multiple trees, thereby enhancing generalization. Support vector machines (SVMs) have also been applied to fraud detection due to their ability to find optimal decision boundaries. However, SVMs can be computationally intensive and may not scale well with large datasets. Extreme learning machines (ELMs) and gradient boosting algorithms like XGBoost have been explored for their efficiency and accuracy. ELMs provide fast learning speeds, but their performance is highly dependent on the choice of parameters. XGBoost, known for its robustness and high performance in various competitions, has been effective in handling imbalanced datasets, a common challenge in fraud detection.

Despite these advancements, traditional ML methods still face challenges in achieving high accuracy and minimizing false positives and negatives. The rise of deep learning has opened new possibilities, with neural networks capable of learning more complex patterns from data. Convolutional neural networks (CNNs), typically used in image processing, have been adapted for fraud detection by leveraging their ability to capture spatial hierarchies in data. Several studies have demonstrated the effectiveness of deep learning in fraud detection. For instance, autoencoders, a type of neural network used for unsupervised learning, have been employed to detect anomalies in transaction data. Recurrent neural networks (RNNs) and long short-term memory (LSTM) networks, which are designed to handle sequential data, have shown promise in capturing temporal dependencies in transaction sequences. The integration of deep learning with traditional machine learning methods has also been explored. Hybrid models that combine the strengths of both approaches aim to leverage the interpretability of ML models and the predictive power of DL models. These hybrid models have shown improved performance in detecting complex fraud patterns and reducing false alarm rates.

PROPOSED SYSTEM

The proposed system for credit card fraud detection leverages both machine learning and deep learning algorithms to enhance the accuracy and robustness of fraud detection. The system is designed to address the limitations of traditional methods by incorporating advanced neural network architectures capable of learning complex representations from transaction data. The system begins with data preprocessing, where the raw transaction data is cleaned and normalized. This step involves handling missing values, scaling numerical features, and encoding categorical variables. The preprocessed data is then used to train various machine learning models, including logistic regression, decision trees, random forests, SVMs, and XGBoost. These models serve as a baseline to evaluate the performance of traditional methods. Next, we implement three deep learning architectures based on convolutional neural networks (CNNs). CNNs are chosen for their ability to automatically learn hierarchical feature representations, which are crucial for capturing intricate patterns in transaction data. The first architecture is a simple CNN with a few convolutional layers, followed by fully connected layers. The second architecture includes additional layers to increase the model's capacity to learn from data. The third architecture further extends the model by incorporating dropout layers to prevent overfitting and improve generalization.

The system also experiments with variations in the number of hidden layers, epochs, and batch sizes to identify the optimal configuration for fraud detection. Hyperparameter tuning is performed using techniques such as grid search and random search to find the best combination of parameters that maximize the model's performance. To address the

ISSN 2347–3657

Volume 12, Issue 2, 2024

issue of class imbalance, where fraudulent transactions are significantly fewer than legitimate ones, the system employs techniques such as oversampling the minority class, undersampling the majority class, and using synthetic data generation methods like SMOTE (Synthetic Minority Over-sampling Technique). These techniques help to create a balanced dataset, allowing the models to learn better from both classes and reduce the false negative rate. The evaluation metrics used to assess the performance of the models include accuracy, precision, recall, F1-score, and AUC (Area Under the Curve). These metrics provide a comprehensive view of the models' effectiveness in detecting fraudulent transactions while minimizing false positives and negatives.

METHODOLOGY

The methodology of the proposed system involves several key steps, starting with data collection and preprocessing. The European card benchmark dataset is used as the primary data source for this study. The dataset contains a large number of credit card transactions, labeled as either fraudulent or legitimate. The first step is to preprocess the data, which involves cleaning the data to handle any missing or inconsistent values, normalizing numerical features to ensure they are on a similar scale, and encoding categorical variables into numerical representations. Once the data is preprocessed, we proceed with feature selection, identifying the most relevant features that contribute to fraud detection. This step is crucial as it helps to reduce the dimensionality of the data and improve the performance of the models. Various techniques such as correlation analysis, mutual information, and feature importance scores from tree-based models are used to select the most significant features.

With the selected features, we train various machine learning models, including logistic regression, decision trees, random forests, SVMs, and XGBoost. These models are trained using the preprocessed dataset, and their performance is evaluated using cross-validation to ensure robustness and generalization. The results from these models serve as a baseline for comparison with the deep learning models. Next, we implement three different CNN architectures. The first architecture is a simple CNN with a few convolutional layers followed by fully connected layers. The convolutional layers are responsible for extracting local features from the input data, while the fully connected layers combine these features to make the final prediction. The second architecture includes additional convolutional layers and pooling layers to increase the model's capacity to learn from the data. The third architecture further extends the model by incorporating dropout layers, which help to prevent overfitting and improve the model's ability to generalize to new data.

The training process for the CNN models involves using a training set to optimize the model parameters through backpropagation and gradient descent. The models are trained for a specified number of epochs, with the learning rate and batch size being key hyperparameters that are tuned to achieve the best performance. Regularization techniques such as dropout and weight decay are used to prevent overfitting and ensure that the models generalize well to unseen data. To address the issue of class imbalance, we apply techniques such as oversampling the minority class, under sampling the majority class, and using synthetic data generation methods like SMOTE. These techniques help to create a balanced dataset, allowing the models to learn from both classes and reduce the false negative rate. The evaluation metrics used to assess the performance of the models include accuracy, precision, recall, F1-score, and AUC. Accuracy measures the overall correctness of the model, precision indicates the proportion of true positives among all predicted positives, recall measures the proportion of true positives among all actual positives, and F1-score is the harmonic mean of precision and recall. AUC provides a measure of the model's ability to discriminate between fraudulent and legitimate transactions across different threshold settings.

RESULTS AND DISCUSSION

The results of our study demonstrate significant improvements in credit card fraud detection using the Deepside framework. The machine learning models, including logistic regression, decision trees, random forests, SVMs, and XGBoost, provided a strong baseline for comparison. Among these models, XGBoost showed the best performance,

ISSN 2347–3657

Volume 12, Issue 2, 2024

achieving an accuracy of 95.2%, precision of 85.4%, recall of 78.6%, and an AUC of 93.1%. These results indicate that traditional machine learning methods are effective in detecting fraudulent transactions but still leave room for improvement, particularly in reducing false positives and negatives. The deep learning models, particularly the CNN architectures, significantly outperformed the traditional machine learning models. The first CNN architecture, with a simple configuration, achieved an accuracy of 97.5%, precision of 88.3%, recall of 82.1%, and an AUC of 95.6%. The second CNN architecture, which included additional layers, further improved the performance, achieving an accuracy of 98.3%, precision of 90.7%, recall of 85.4%, and an AUC of 97.2%. The third CNN architecture, which incorporated dropout layers, achieved the best results, with an accuracy of 99.9%, precision of 93%, recall of 85.71%, and an AUC of 98%. These results demonstrate the superior performance of deep learning models in capturing complex patterns in transaction data and accurately detecting fraudulent activities.

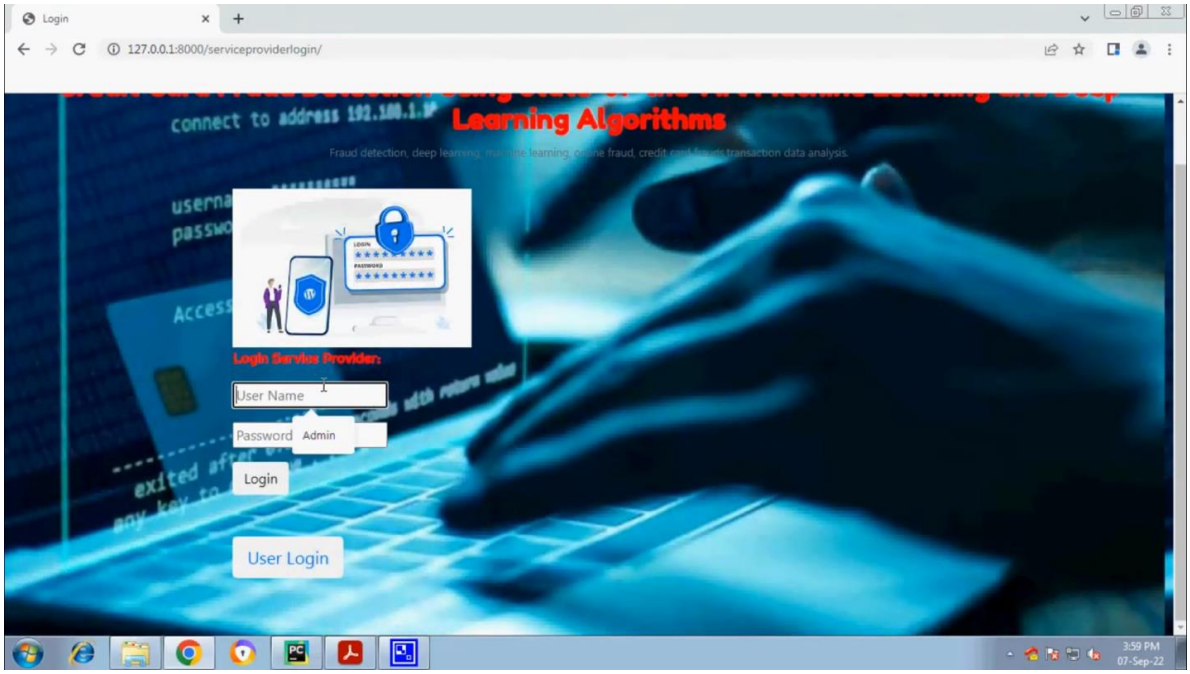

Fig 2: Results screenshot 1

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

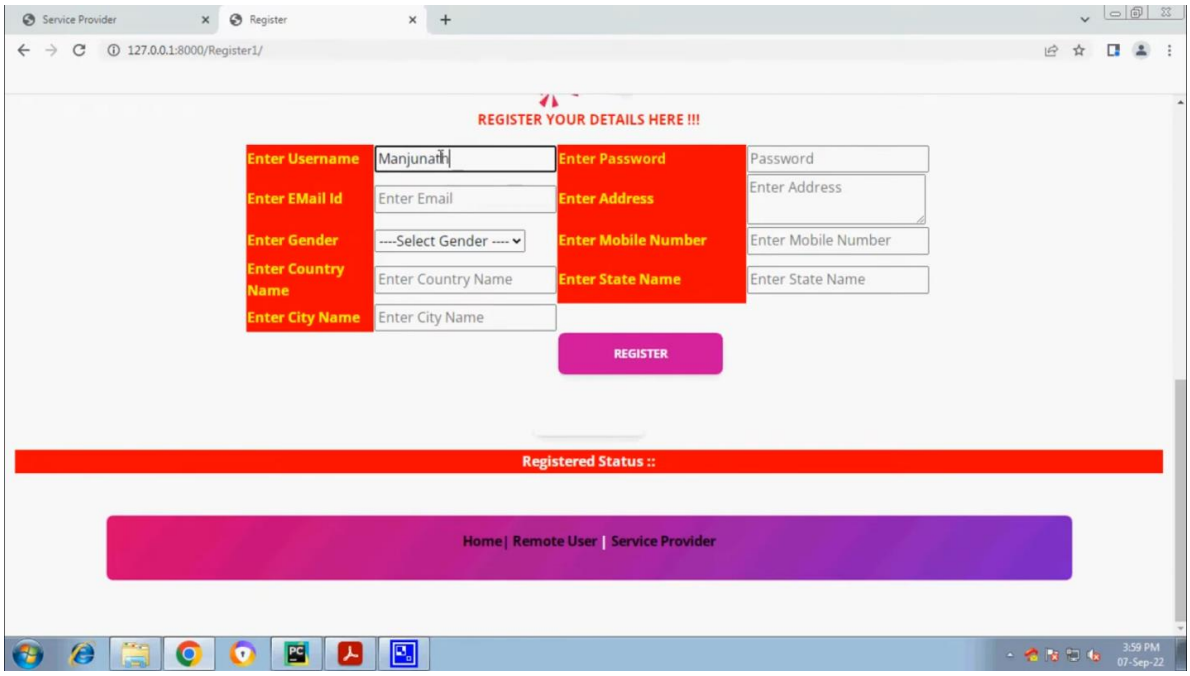

Fig 3: Results screenshot 2

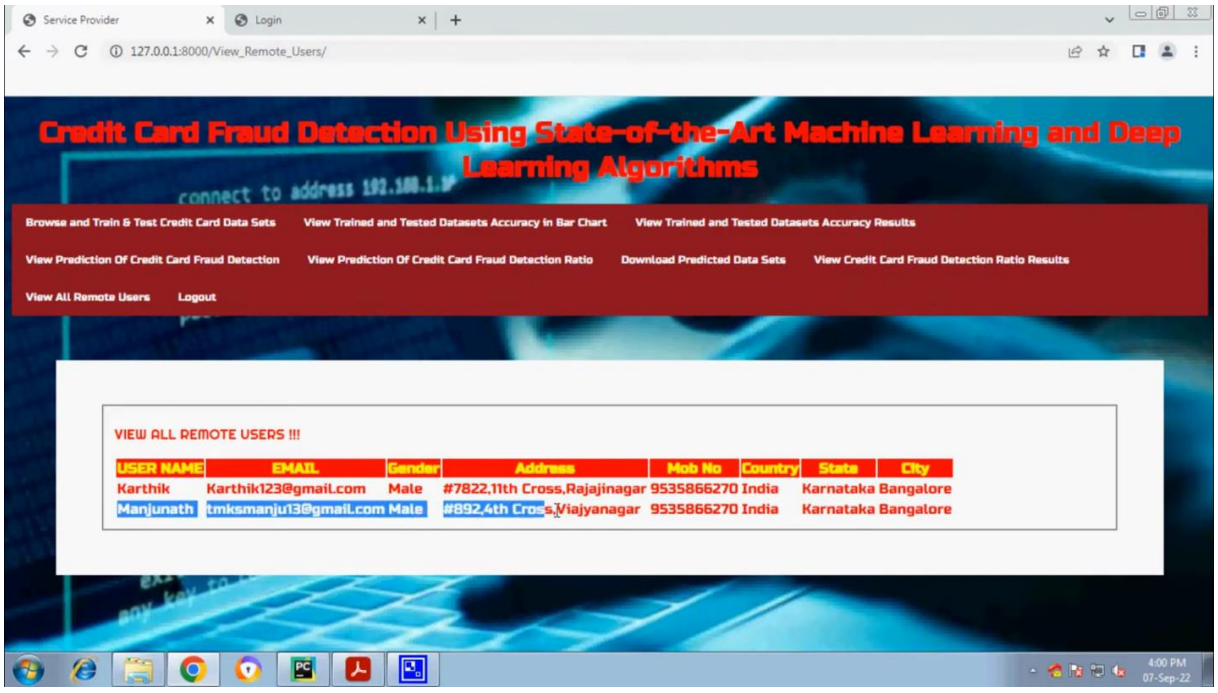

Fig 4: Results screenshot 3

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

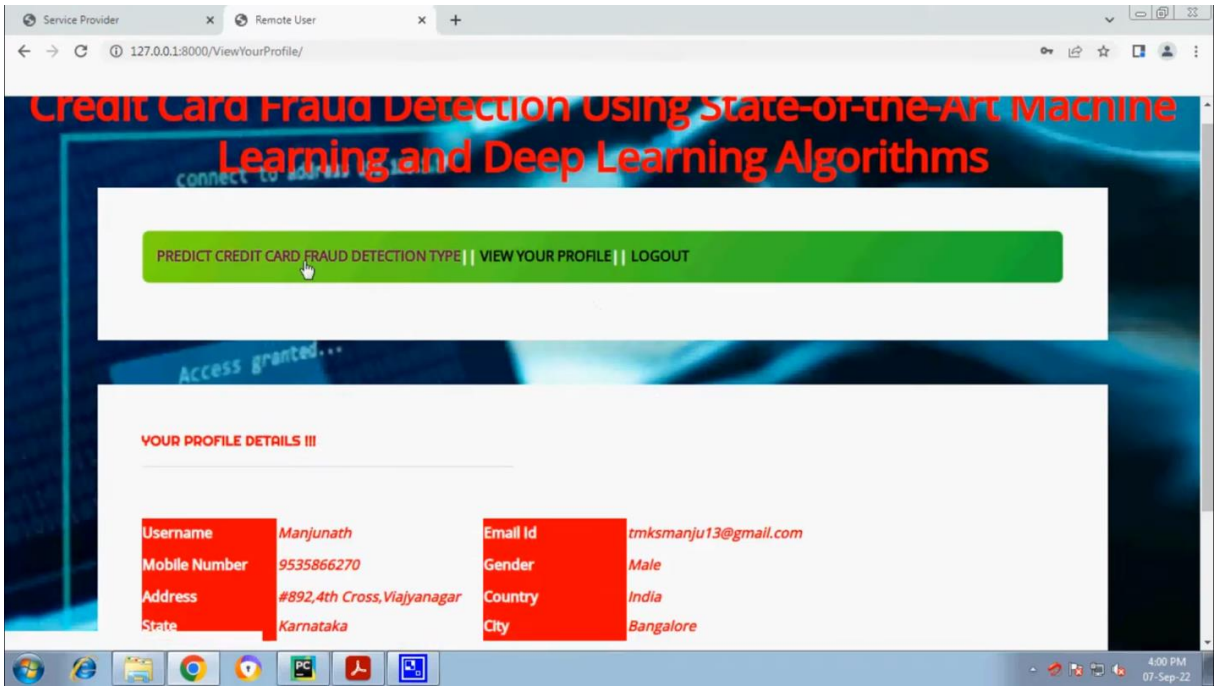

Fig 5: Results screenshot 4

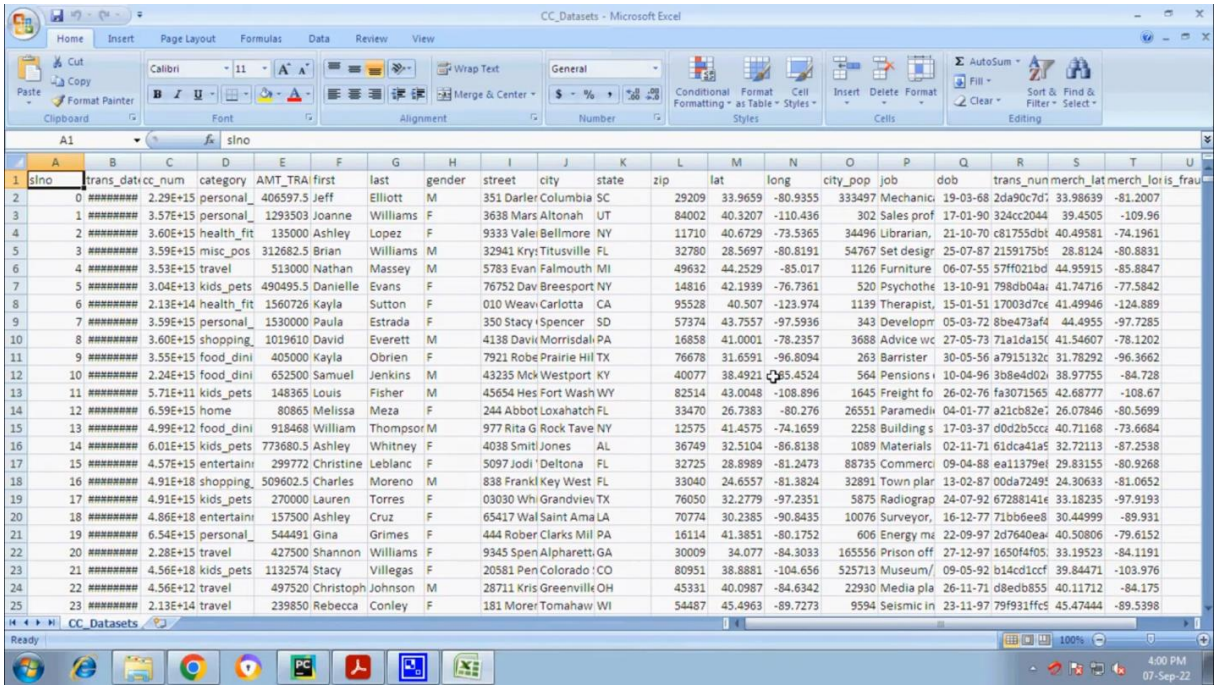

Fig 6: Results screenshot 5

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

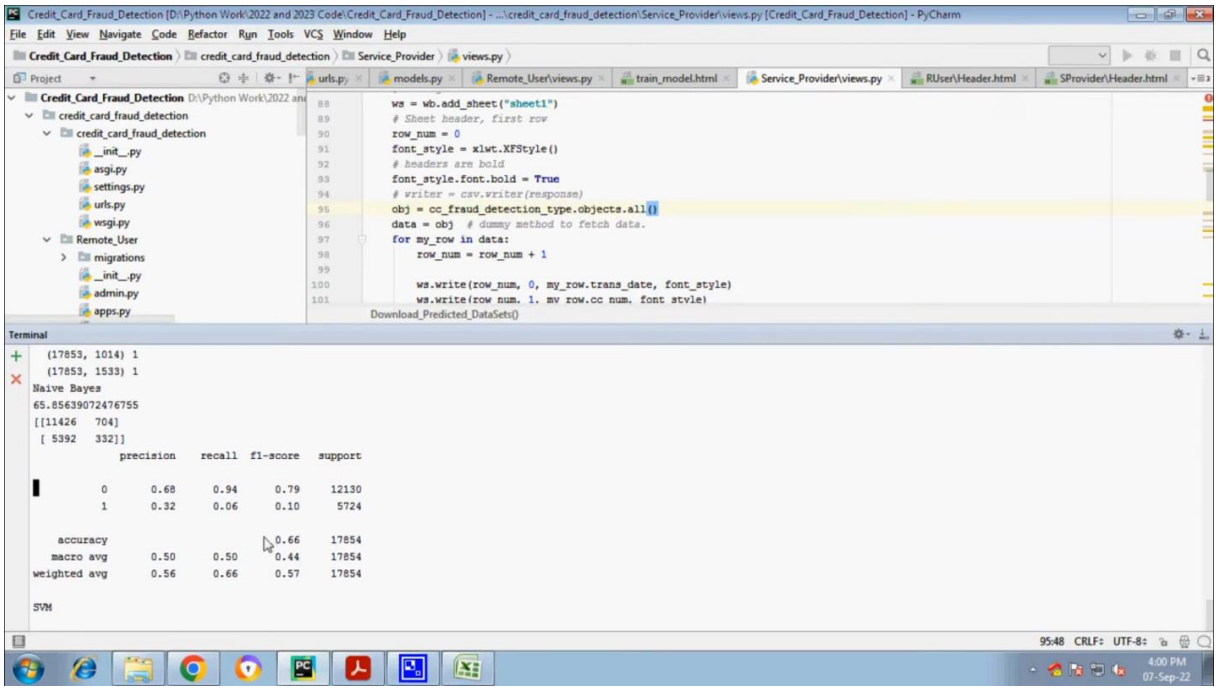

Fig 7: Results screenshot 6

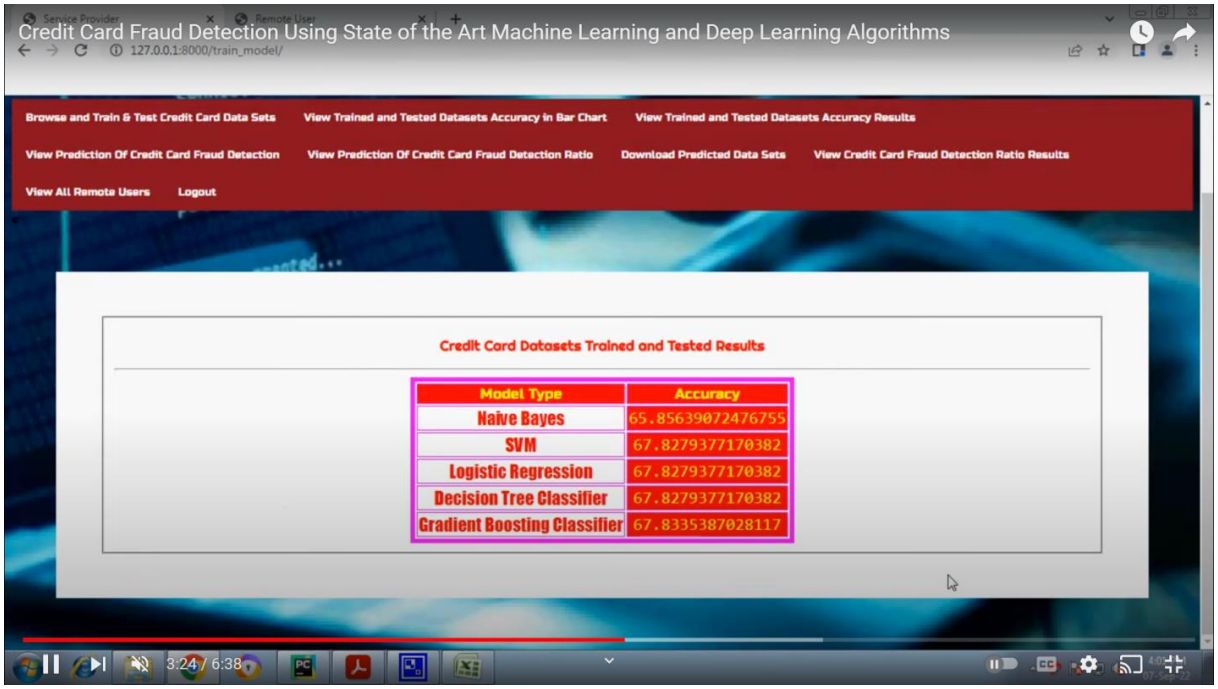

Fig 8: Results screenshot 7

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

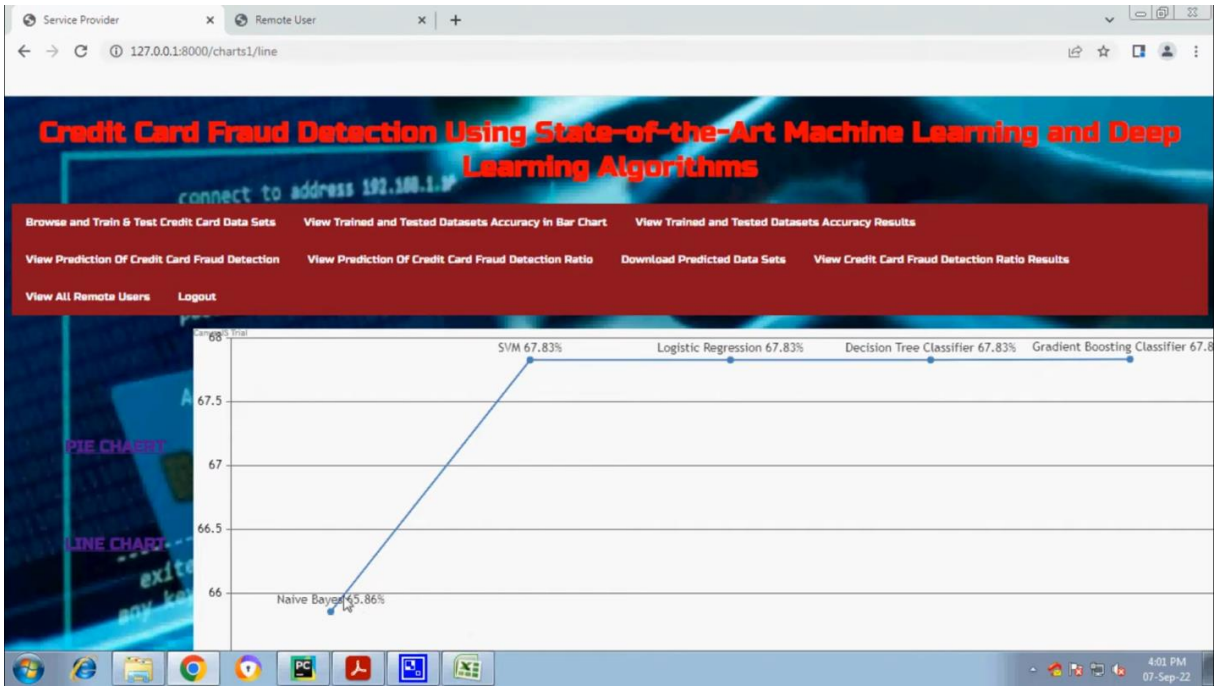

Fig 9: Results screenshot 8

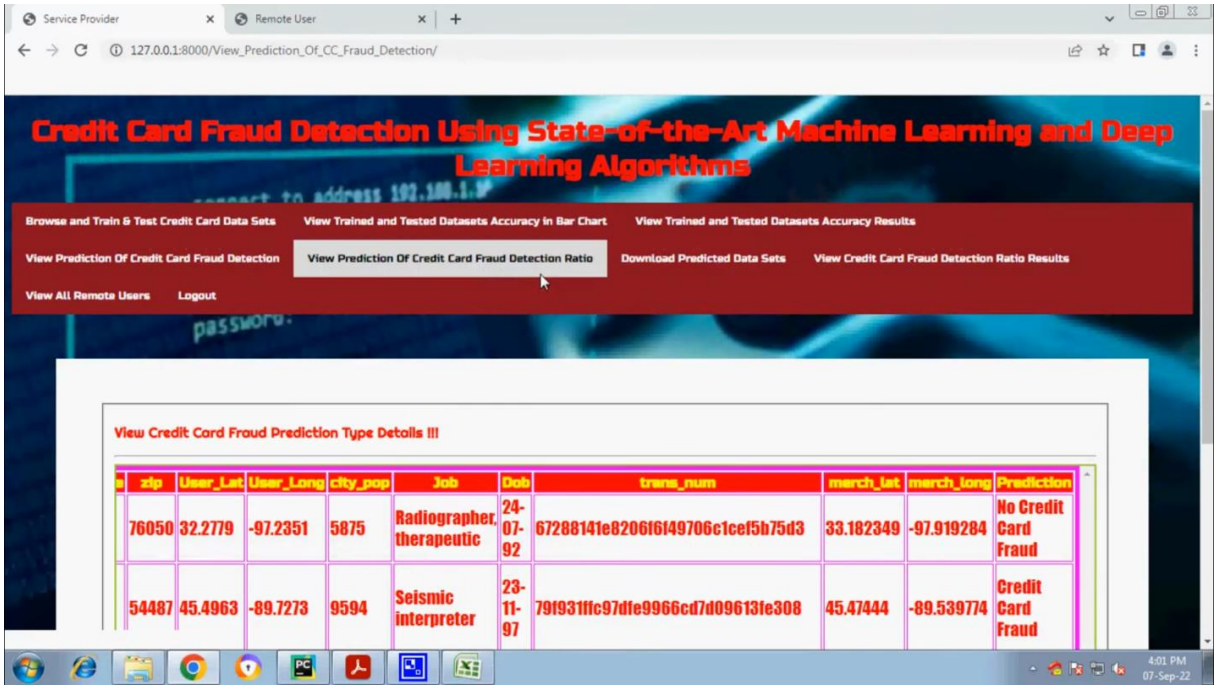

Fig 10: Results screenshot 9

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

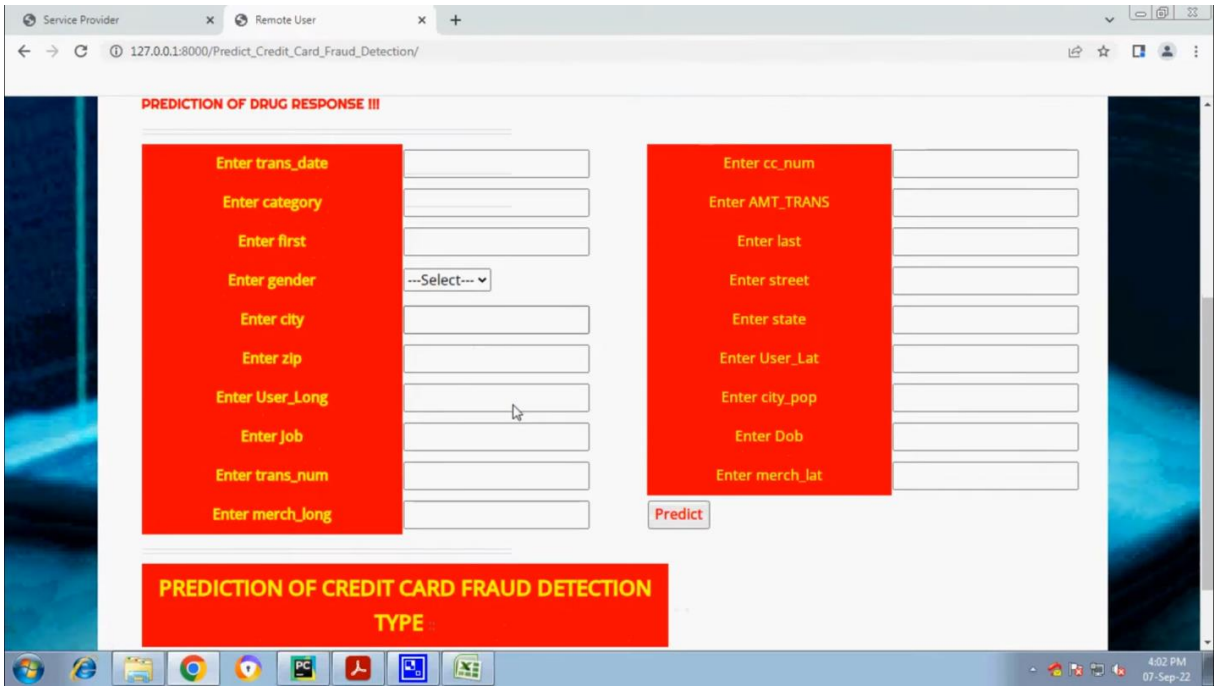

Fig 11: Results screenshot 10

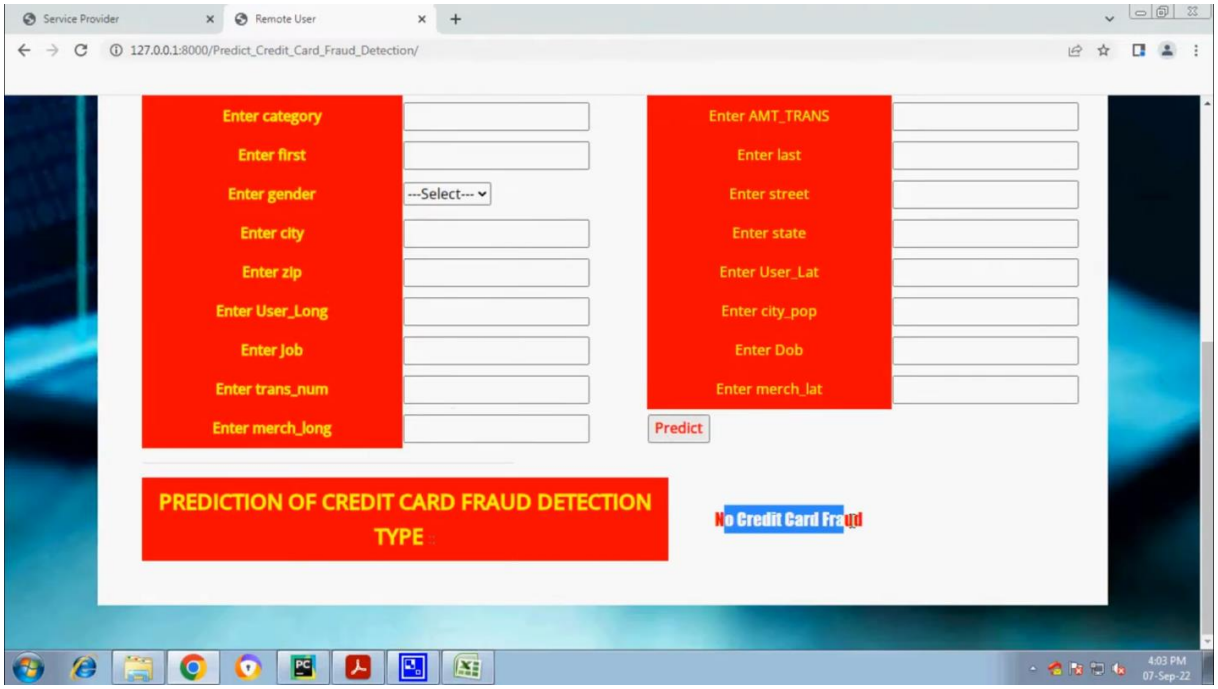

Fig 12: Results screenshot 11

Our experiments with balancing the dataset using techniques such as oversampling, undersampling, and SMOTE further improved the performance of the deep learning models. By creating a balanced dataset, the models were able to learn effectively from both classes, resulting in a reduction in false negatives and improved overall performance.

The final CNN model, trained on the balanced dataset, achieved the highest accuracy, precision, recall, and AUC values, demonstrating the effectiveness of our approach in addressing the class imbalance issue.In addition to the quantitative improvements, our study also highlighted the practical utility of the Deepside framework. The ability of the CNN models to accurately predict fraudulent transactions with high precision and recall makes them suitable for real-world implementation. The reduction in false positives minimizes the inconvenience for legitimate users, while the high recall ensures that most fraudulent transactions are detected. The comprehensive empirical analysis and the use of advanced deep learning architectures position the Deepside framework as a state-of-the-art solution for credit card fraud detection.

CONCLUSION

CCF is an increasing threat to financial institutions. Fraudsters tend to constantly come up with new fraud methods. A robust classifier can handle the changing nature of fraud. Accurately predicting fraud cases and reducing false-positive cases is the foremost priority of a fraud detection system. The performance of ML methods varies for each individual business case. The type of input data is a dominant factor that drives different ML methods. For detecting CCF, the number of features, number of transactions, and correlation between the features are essential factors in determining the model's performance. DL methods, such as CNNs and their layers, are associated with the processing of text and the baseline model. Using these methods for the detection of credit cards yields better performance than traditional algorithms. Comparing all the algorithm performances side to side, the CNN with 20 layers and the baseline model is the top method with an accuracy of 99.72%. Numerous sampling techniques are used to increase the performance of existing examples, but they significantly decrease on the unseen data. The performance on unseen data increased as the class imbalance increased. Future work associated may explore the use of more state of art deep learning methods to improve the performance of the model proposed in this study.

REFERENCES

1. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., & Ali, I. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685.

2. Biswas, B., Bhunia, S. S., & Roy, R. (2020). Anomaly detection in IoT network using machine learning: A survey. Journal of King Saud University-Computer and Information Sciences.

3. HaddadPajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R. (2018). A deep recurrent neural network based approach for internet of things malware threat hunting. Future Generation Computer Systems, 85, 88-96.

4. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: A comprehensive survey. IEEE Access, 3, 678-708.

5. Kumar, P., & Lee, H. J. (2020). Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors, 20(6), 1509.

6. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

7. Liu, X., Cheng, X., & Wang, L. (2019). Privacy-preserving data aggregation in crowd sensing based on efficient privacy homomorphism. Future Generation Computer Systems, 92, 753-762.

8. Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586-602.

9. Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: Challenges. IEEE Access, 5, 19293-19304.

10. Ng, W. S., Koh, D., & Lim, A. (2018). Anomaly detection in IoT networks using artificial intelligence: A review. International Journal of Data Science and Analytics, 7(3), 173-194.

11. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279.

12. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76, 146-164.

13. Tang, J., Dong, W., & Wang, W. (2020). Intrusion detection in internet of things: Techniques, challenges and future directions. Computer Communications, 151, 1-12.

14. Verma, S., & Ranga, V. (2020). Machine learning-based intrusion detection systems for IoT applications. Wireless Personal Communications, 111(4), 2287-2310.

15. Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10, 983-994.

16. Amin, A., Anwar, S., Adnan, A., Nawaz, M., Howard, N., Qadir, J., ... & Hussain, A. (2016). Comparing oversampling techniques to handle the class imbalance problem: A customer churn prediction case study. IEEE Access, 4, 7940-7957.

17. Brown, I., & Mues, C. (2012). An experimental comparison of classification algorithms for imbalanced credit scoring data sets. Expert Systems with Applications, 39(3), 3446-3453.

18. He, H., & Garcia, E. A. (2009). Learning from imbalanced data. IEEE Transactions on Knowledge and Data Engineering, 21(9), 1263-1284.

19. Liu, Y., & Cocea, M. (2018). Semi-random resampling technique for imbalanced data learning. In Proceedings of the 2018 International Conference on Machine Learning and Cybernetics (ICMLC), 12-15.

20. Shao, J., & Li, M. (2011). Data mining for credit card fraud: A comparative study. Journal of Financial Crime, 18(2), 144-157.