Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

Cloud-Based AI solutions for credit card fraud detection with feedforward neural networks in banking sector

[1]Charles Ubagaram , [2]Karthick.M

[1]Tata Consultancy Services,Ohio,USA
[2]Nandha College of Technology, Erode

[1]charlesubagaram17@gmail.com

[2]magukarthik@gmail.com

Abstract- The increasing complexity of fraud strategies, combined with the rapid increase in transaction volumes, makes credit card fraud detection an important area of consideration in the banking sector. Due to the complexities of fraudulent behavior in the context of large transaction sizes, traditional techniques for fraud detection based on rules have become incapable of meeting the challenge. Cloud-based AI solutions based on Feedforward Neural Networks (FNNs) provide the best option when looking for an advanced adaptive approach. This solution benefits from cloud storage to provide highly efficient management of large volumes of transactional data with maximum scalability and flexibility. FNNs aid in differentiating and recognizing complex fraud patterns, while cloud technology ensures that such a system is proficient in adjusting to transaction volume fluctuations. The integration of these technologies resulted in the model achieving a 99.89% accuracy, 98.67% precision, and 95.76% recall. The F1-score of 96.78% shows a balanced performance in precision versus recall. This convergence of AI and cloud technologies promotes accurate fraud transaction detection with reduced false-positive responses and the possibility of continuous adaptation to new fraud schemes. All said, Cloud-Based AI with FNNs is a system that is most potent to secure financial transactions and customers' interests in the banking sector.

Keywords: Feedforward Neural Networks, Banking Sector, Fraud Detection Systems, Transaction Data, Cloud-Based AI

1. Introduction

Credit card fraud has emerged as a major concern for the financial sector, causing significant economic losses and eroding consumer confidence [1]. The increasing frequency and sophistication of fraudulent transactions underscore the need for advanced fraud detection methods [2]. Fraudulent activities typically involve unauthorized access to sensitive credit card information, which results in illegal purchases [3]. These criminal acts compromise the integrity and trustworthiness of digital payment infrastructures [4]. Financial institutions face substantial challenges in combating these threats while maintaining seamless user experiences [5]. Traditional rule-based fraud detection systems, though effective to some extent, lack the agility to deal with dynamic fraud patterns [6]. Many of these methods depend heavily on predefined heuristics that are often inadequate against novel or evolving fraud tactics [7]. The rapid proliferation of online banking and digital transactions has further complicated fraud detection processes [8].

A key contributor to credit card fraud is the widespread availability of personal data on public and dark web platforms [9]. Weak security frameworks and insufficient authentication mechanisms leave users vulnerable to identity theft and misuse [10]. Fraudsters commonly exploit stolen credit card numbers obtained through data

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

breaches and skimming devices [11]. Social engineering techniques and phishing campaigns are also prevalent attack vectors used to deceive unsuspecting individuals [12]. The advent of e-commerce has expanded the attack surface for cybercriminals, enabling fraudulent activities across multiple platforms [13]. Recent developments in AI have shown promise in addressing these challenges by learning from vast historical transaction datasets [14]. However, the increasing complexity of fraud tactics makes it difficult to reliably identify illicit activities in real-time [15]. Most traditional systems still rely on linear, rule-based logic that struggles to adapt to rapidly changing threat landscapes [16].

Despite technological advancements, several limitations in existing detection systems persist [17]. High false positive rates continue to plague current solutions, leading to customer dissatisfaction and service disruption [18]. Misclassification of legitimate transactions as fraudulent incurs unnecessary operational costs for financial institutions [19]. The trade-off between sensitivity and specificity in detection models is a persistent design challenge [20]. Scalability also remains an issue, as many legacy systems cannot effectively process large-scale transactional data [21]. Furthermore, the imbalanced nature of credit card datasetswhere fraudulent cases form a minor fractionposes a hurdle for machine learning models [22]. This imbalance often results in biased models that fail to accurately detect rare fraud instances [23]. Consequently, conventional fraud detection systems remain vulnerable to evolving and adaptive threats [24].

There is a pressing need for next-generation approaches that are both flexible and intelligent in identifying suspicious behaviour [25]. Incorporating AI and cloud-based frameworks can enhance detection capabilities by enabling real-time analytics and adaptive learning [26]. Cloud computing offers scalable resources to manage high-throughput transaction streams efficiently [27]. Moreover, distributed AI systems facilitate collaborative fraud detection across different organizational nodes [28]. Machine learning algorithms can uncover hidden patterns in large datasets that traditional methods often overlook [29]. Deep learning techniques, such as neural networks, provide powerful tools for modelling complex, non-linear transaction behaviours [30]. Feature engineering and selection play critical roles in improving model interpretability and performance [31]. Unsupervised learning methods are particularly useful in identifying previously unseen fraud types [32].

Meanwhile, ensemble models combine multiple classifiers to boost accuracy and reduce variance in predictions [33]. Time-series analysis and sequential modelling are also employed to detect anomalies in transaction sequences [34]. Reinforcement learning has shown potential in dynamically optimizing fraud detection policies based on feedback [35]. Data privacy and security must be maintained when deploying AI models in sensitive financial environments [36]. Techniques such as federated learning allow model training without centralized access to raw customer data [37]. Explainable AI is gaining traction to ensure transparency and regulatory compliance in automated decision-making [38]. Real-time dashboards and visualization tools support rapid response to emerging fraud trends [39]. Continuous model evaluation and updates are necessary to maintain relevance against adaptive adversaries [40]. Benchmarking against publicly available fraud datasets enables objective comparison and validation of new approaches [41]. This research presents a comprehensive fraud detection framework that leverages cloud infrastructure and AI techniques to build robust, scalable, and adaptive credit card fraud detection systems [42].

- Adopted for the detection of credit card fraud in banks, utilizes Cloud-based AI solutions, particularly FNN.
- Improves the accuracy of identifying fraudulent transactions and reduces the number of incorrect fraud alerts.
- The model is flexible enough to adapt to the newly emerging patterns of fraud and thus improves its detection capabilities with time.

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

- When there is need to store bulk transactional data, going for such a cloud-based approach becomes a very scalable and cost-effective solution.
- It ensures the security of transactions or dealings in finances and protects customers' data from fraud.

The paper is structured as follows: Section 1 presents the introduction and literature review, Section 2 describes the proposed methodology, Section 3 discusses the results and analysis, and Section 4 provides the conclusion and suggestions for future work.

2. Literature survey

An IoT-based structural health monitoring (SHM) system has been shown to support damage detection using cross-correlation methods, with noise reduction achieved via Butterworth filtering [43]. Mathematical modeling techniques are used to determine the extent and location of the damage within structural systems monitored by IoT frameworks [44]. Wireless sensor networks enable the deployment of numerous small sensors, making large-scale IoT applications viable in fields such as smart traffic systems, environmental monitoring, and infrastructure management [45]. An IoT-driven healthcare framework utilizing ECG sensors and Hidden Markov Models (HMM) has been developed for managing cardiovascular diseases, enhancing real-time patient tracking, alert systems, and location awareness [46]. A mathematical framework involving piezoelectric sensors and a Raspberry Pi has been proposed for IoT-based SHM to localize and detect structural anomalies [47].

A low-cost and robust IoT architecture for real-time vehicle tracking has been developed using RFID sensors and velocity estimation through Euler's methods, outperforming traditional image processing systems due to the detection capabilities of RFID [48]. Embedded web servers have been utilized for real-time control of appliances and machinery over the Internet, supporting industrial automation through IoT integration [49]. A cost-effective health monitoring platform was proposed as part of an IoT healthcare system for rural deployment, allowing for continuous tracking of medical parameters and facilitating remote communication between patients and medical professionals [50]. A wearable biosensing mask leveraging surface electromyography (sEMG) was designed for pain intensity monitoring and can be integrated with IoT systems for low-power, real-time remote analysis [51].

IoT-enabled systems have been employed in proactive healthcare analytics and anomaly detection, especially for heart disease prevention through real-time data monitoring and pattern recognition [52]. Compression techniques for sensor data were investigated to reduce information loss while maximizing efficiency in data transmission, enabling better resource management in IoT-based systems [53]. A cloud-integrated IoT solution has also been created for ECG wave visualization through an Android application, allowing users to log and analyze heart activity in real time [54]. Furthermore, an IoT-based wearable ECG diagnostic device employing Discrete Wavelet Transform (DWT) and Support Vector Machine (SVM) enables continuous 24/7 heartbeat monitoring and arrhythmia detection [55].

These advancements demonstrate how SHM systems benefit from both low-cost hardware and advanced analytics for remote monitoring and real-time diagnostics [56]. IoT solutions now allow dynamic reconfiguration of embedded sensors to optimize data acquisition based on health event triggers [57]. Wearable health devices increasingly leverage multimodal sensors for capturing complex physiological events like seizures and arrhythmias [58]. Feature extraction methods such as time-frequency analysis have been critical for accurately identifying events in real-time biomedical systems [59]. Edge computing platforms that integrate with IoT sensors offer immediate feedback, enhancing patient outcomes through prompt intervention

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[60]. The integration of machine learning algorithms on embedded devices allows predictive modelling without cloud reliance [61].

Low-power transmission protocols such as LoRa and BLE are commonly used to reduce energy consumption in IoT healthcare deployments [62]. Seamless interoperability between devices and cloud platforms has become a focal point in designing scalable healthcare IoT infrastructures [63]. Security and privacy remain essential challenges as sensitive physiological data is continuously streamed and processed across networks [64]. Modular IoT architectures ensure adaptability for expanding system functionalities as medical technologies evolve [65]. Cross-platform compatibility in mobile health systems ensures broader user access to real-time diagnostic tools and monitoring apps [66]. The continued refinement of signal pre-processing techniques, wearable hardware, and AI inference pipelines will play a vital role in the future of IoT-based biomedical systems [67].

2.1 Problem statement

Mobile broadband explosion created differences in the area of financial inclusion and e-commerce, particularly for rural areas, thus influencing socioeconomic growth[68]. An efficient and scalable solution that combines cutting-edge technologies that include Deep AR-based time series forecasting, Neural Turing Machine, and Quadratic Discriminant Analysis to ameliorate the situation should be in place[69]. One of the main issues in the banking industry is the detection of credit card fraud, for which Cloud-Based Artificial Intelligence solutions with FNN support would identify fraudulent transactions nearly[70]. The company would use machine learning merging with probabilistic models to reject false positives cost-effectively, despite the financial data being noisy, of high dimensionality, and non-linear[71]. The solution seeks to integrate AI, Big Data, and IoT technologies for predictive analytics improvement, resource use, and scalability while ensuring secure and efficient transaction processing in the financial sector[72].

3. Proposed Methodology

The flowchart gives a pictorial description of the technique of detecting fraudulent transactions in the banking sector using a cloud-based FNN. The first step involves collecting the necessary data on transactions, such that the acquired data is subjected to pre-processing phases that start with normalization and SMOTE. Normalization means scaling all the numerical features in relation to one another such that the neural network model can carry them forward for computation. SMOTE is a technique that helps in generating synthetic instances of the minority class, namely fraudulent transactions, to take care of the issues regarding class imbalance. The final stage is classification, where the FNN model processes the transactions and gives an assessment on whether they are classified as fraud detected or not detected. Results from the model are stored in cloud storage for easy retrieval and scalability in the future.Thus, storage and management of part of a larger dataset is rendered easy since it runs on cloud technology. This structure offers mobile, flexible responsiveness in the management of large transaction volumes as well as the incorporation of new and varying data. Scalable and proficient cloud technology is offered by AI fraud detection in the eradication of fraud in terms of accuracy.

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

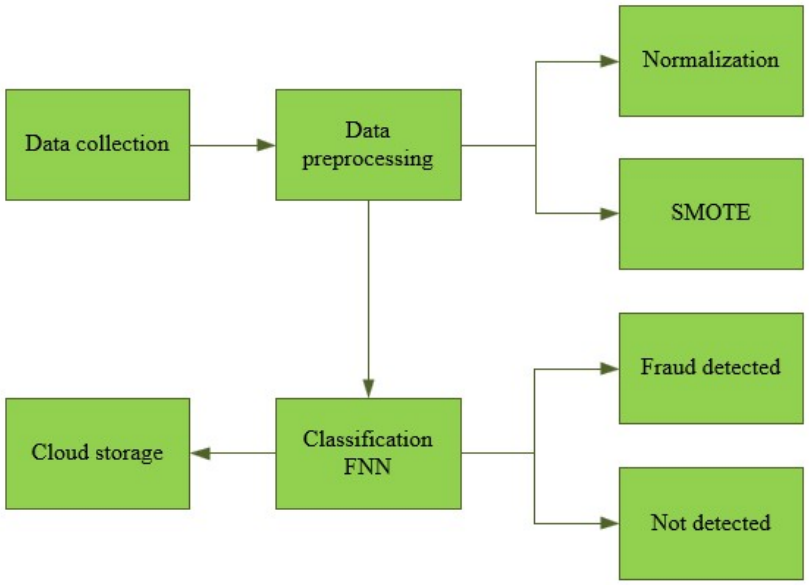

Figure 1: Architecture diagram of proposed methodology

3.1 Data collection

The dataset Credit card fraud detection includes, transaction data from a brief period and highly imbalanced between the fraudulent and non-fraudulent transactions it contains. It includes only numerical features that came except for time and amount features. The first time a transaction happened, and the amount any later transaction was worth did pose a great deal of significance.The class variable indicates whether the transaction is considered fraudulent or not.

3.2 Data pre-processing

Data pre-processing comprises an important step to enhance the dataset for training deep learning models. Data processing, for instance, helps to normalize features such as Amount and Time to a unified scale, making it simpler to learn through these elements. One of the key steps in data processing would be imbalance handling, which fixes issues using SMOTE or under-sampling, for example, to get the classes fraudulent versus non-fraudulent as a balance and not allowing the model to give preference to the majority class. Then, the processed data is used to train the classification model and afterward stored in cloud storage for further processing and analysis.

3.2.1 Normalization

Normalization is always making numerical features to a common scale, therefore, be compliant with the analysis or model-building process. This is quite critical that use distance metrics or gradient descent, since unequal measurements in the measurement scales will give rise to different performance results. The min-max technique combines feature values in the range, which is usually between 0 and 1, by subtracting the minimum value and dividing by the range. One other familiar way of scaling value is z-score standardization that centers data at a mean of 0 and a standard deviation of 1. Normalization enables the model to perform better and be more stable in cases during training because with normalization, all input features will be in comparable scales, even though some may have different units or ranges. Min-max normalization is a common normalization procedure that scales data using the following equation (1):

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (1)$$

where, x' is the normalized value, x is the original value of the feature, $\min(x)$ is the minimum value of the feature in the dataset, $\max(x)$ is the maximum value of the feature in the dataset. This formula scales all feature values into the range from 0 to 1, where the minimum value is mapped to 0 and the maximum value is mapped to 1.

3.2.2 SMOTE

The SMOTE (Synthetic Minority Over-Sampling Technique) is a common technique for creating synthetic samples for the minority class as opposed to duplicate samples from it, with the aim of achieving balance in a data set. The application of SMOTE involves choosing a data point from the minority class and then computing the k nearest neighbors of that data point from the same class. Out of these neighbors, one is chosen randomly, and a synthetic instance is created along the line segment joining the two points. The generation of new samples is given by the equation (2):

$$x_{new} = x_i + \delta \cdot (x_{zi} - x_i) \quad (2)$$

where, x_i is an existing sample. δ is a random number between 0 and 1, used to control how far the synthetic point is between x_i and x_{zi}. $x_{zi} - x_i$ calculates the difference between the neighbor and the original point. $\delta \cdot (x_{zi} - x_i)$ scales the vector by a random amount, giving a point somewhere along the line between x_i and x_{zi}. x_{new} final synthetic sample, created by adding the scaled vector to x_i.

3.3 Classification using Feed-Forward Neural Network (FFN)

This is how classification is done on a neural network that has a feed-forward architecture model. The inputs go directly through several interlinked input hidden and output layers. FFN is a uni-directional features that enter through an input layer and outputs to one or many hidden layers to the output layer. The different layers have at least one hidden layer, which associates one or more activation functions through which a set of weighted connections learns how to model inputs into the unary output form final output into the output layer as a probability distribution over possible class output. Each neuron receives input from the previous layer neuron, applies an activation function together with some transforms to the inputs, and feeds it to a next layer neuron. Instead of generating outputs directly, outputs from the output layer use a function similar to SoftMax to derive probabilities for each class, which now enables the network to finalize a prediction. Comparing with the true label over time gives the output the immediate value it obtained after processing the inputs using a loss function like cross-entropy. The value brought forth by the model is then used for modification of weights through backpropagation and possibly some optimization method like gradient descent.

- **Input Layer:**

It's the first layer in an FNN where the data enters the system. The input layer receives the feature vector of each data sample and passes it on to the next layer without changing or activating it itself.The input to the network is represented in equation (3):

$$\mathbf{x} = [x_1, x_2, \ldots, x_n]^T \quad (3)$$

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

Where, $\mathbf{x}$ is the input vector, x_i is value of the i^{th} feature.

- **Hidden layer**

Hidden layers of anFNN are the key learning areas whereby the network learns to sense patterns, relationshipsfrom the input data. Each hidden layer consists of neurons. **compute the output of a hidden layer**in a**FFN is shown in equation (4)**

$$a^{(l)} = f\left(W^{(l)} \cdot a^{(l-1)} + b^{(l)}\right) \quad (4)$$

Where, $a^{(l)}$ is the output of the current hidden layer l, $W^{(l)}$ is the weight matrix connecting the previous layer to this layer, $a^{(l-1)}$ is the output from the previous layer, $b^{(l)}$ is the bias vector added to the weighted sum

- **Output layer**

The output layer generates the final prediction in a feed. The raw score is passed through a SoftMax function to convert it into class probabilities, calling for multi-classing on the basis of the one that gets the highest probability output**.**The logits are converted into class probabilities using the SoftMax function is showed in equation (5):

$$\hat{y}_i = \frac{e^{z_i}}{\sum_{j=1}^{C} e^{z_j}}, i = 1,2,\dots,C \quad (5)$$

Where, z_i is the logit for class i,$\hat{y}_i$ is the predicted probability for class i. The output layer is the last layer that generates predictions. The predicted class is the one with the highest probability.

3.4 Cloud storage

Cloud storage forms the backbone of Cloud-Based Artificial Intelligence systems for detecting fraud in credit card transactions within the banking sector. The fact that it has a flexible infrastructure that can hold extremely large amounts of transactional data generated, makes it a valuable resource in supporting the dynamicity and ever-increasing nature of bank transactions. Cloud storage provides easy access to data from different locations for analysis of transactions, allowing the detection of fraud as it occurs. Flexible cloud storage integrates these tools easily with other cloud-based tools,smooth data management, processing, and model training becomes possible. In addition, it is scalable, meaning that banks can keep up with the increasing amount of data without investing in costly physical structures. The coset-effectiveness, the payasyougo pricing model-optimizes the operating costs on resource management while promoting efficiency. The cloud storage offers the safest and most reliable storage of sensitive customer data, which, in turn, maintains the bank's privacy as well as compliance with regulations needed in the banking sector.

4. Result and discussion

The fraud detection model performed excellently in terms of various evaluation methodologies. The model captured a high percentage of the fraud while maintaining an excellent false-positive rate, thus preventing inconveniences for most legitimate transactions. It was strong on recall, thus ensuring that most fraudulent activities were detected, and the balance between precision and recall spoke for an optimum model, making it a very reliable fraud detection tool for banking applications. The confusion matrix also indicated that the model is suitable for the correct classification of transactions according to whether they are fraudulent or not.

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

Although the model is heavily challenged by issues like class imbalance and the nature of financial data, it remains a fairly scalable solution for fraud detection because it can learn and adapt to new patterns of fraud.

4.1 Performance analysis

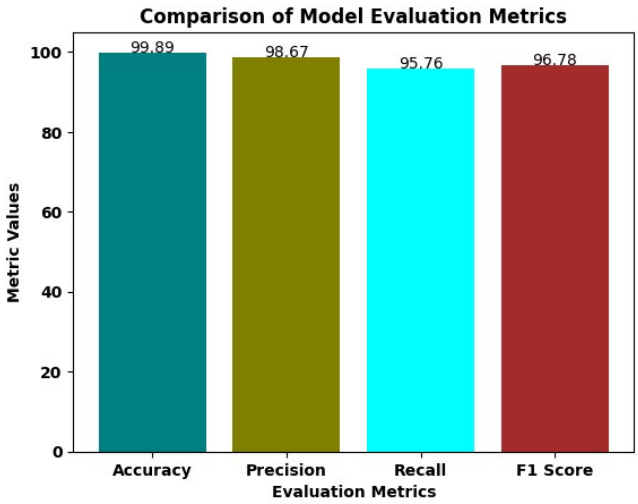

Figure 2: Performance Metrics

The bar graph represents the comparative analysis of the four main evaluation metrics of models. The model performance is outstanding, with a 99.89% accuracy, which indicates that almost all predictions were correct. A Precision of 98.67%, which means very few false positive errors were committed by the model. Recall states that 95.76%, which says that most of the actual positive cases were recognized properly. The F1 score of 96.78%, which indicates that the precision and recall are strongly balanced. This type of consistently high values across such metrics shows that the model is well tuned, highly capable, and robust for classification tasks, making it viable for implementation.

4.2 Confusion Matrix

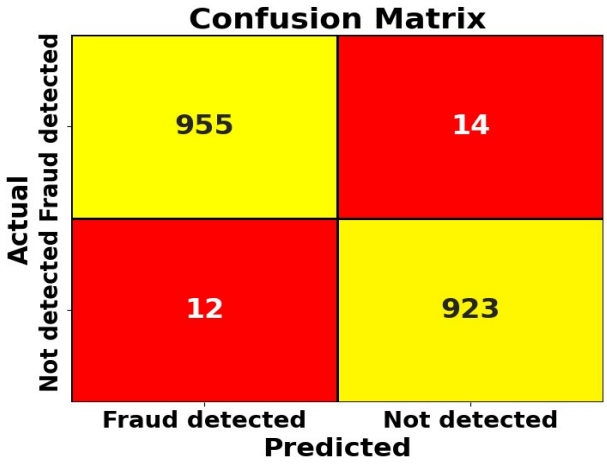

Figure 3: Confusion Matrix

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

The matrix depicts how all outputs are classified either into a positive or negative class through a comparison of the actual values with predicted values in a binary classification model. It shows that the upper left cell of 955 true identifies non-fraud transactions as non-fraud transactions. While the right upper cell of 14 indicates that the non-fraud transactions are falsely classified under fraud, the left lower cell of 12 indicates the false negatives, where fraudulent transactions were classified as non-fraudulent. The bottom right cell of 923 indicates the true positives, wherein the fraudulent transactions were correctly classified as fraudulent. Therefore, the matrix assesses model performance in terms of reducing false positives and false negatives in sensitive systems such as fraud detection.

5. Conclusion

This patent is a Cloud-based AI empowerment offers an economically viable solution to the threat posed by credit card fraud in banks through FNN. With AI cloud-integrated, the system can perform large volumes of transactional data, thus complementing scalability with the requirements of the increasing demand of modern banking. This model yielded a phenomenal 99.89% accuracy whereby almost all transactions were correctly classified. Besides, it achieved 98.67% Precision guaranteeing very few false positives and 95.76% Recall concerning the measure with which fraudulent transactions got identified. The F1 score of 96.78% manifests a very good ratio between precision and recall. FNN can therefore adequately learn on all the strange behaviours hidden in the shadows of the transactional data as far as new and changing trends of fraud detection and prevention are concerned with the recognition of complex patterns that it offers. Moreover, a good, cost-effective option for data stewards is using cloud management, which integrates well with other cloud-based tools and services for seamless access. The technologies, therefore, assure a secure, reliable, and scalable answer for the financial institutions concerning customer interests and integrity protection of the banking system.

References

[1] Barker, K. J., D'amato, J., & Sheridon, P. (2008). Credit card fraud: awareness and prevention. Journal of financial crime, 15(4), 398-410.

[2] Mohanarangan, V.D (2020). Improving Security Control in Cloud Computing for Healthcare Environments.Journal of Science and Technology, 5(6).

[3] Celestin, M., & Vanitha, N. (2019). Ethics in auditing: Addressing conflicts of interest in a complex business landscape. International Journal of Advanced Trends in Engineering and Technology, 4(2), 52-59.

[4] Ganesan, T. (2020). Machine learning-driven AI for financial fraud detection in IoT environments. International Journal of HRM and Organizational Behavior, 8(4).

[5] Georgieva, S., Markova, M., & Pavlov, V. (2019, October). Using neural network for credit card fraud detection. In AIP Conference Proceedings (Vol. 2159, No. 1). AIP Publishing.

[6] Deevi, D. P. (2020). Improving patient data security and privacy in mobile health care: A structure employing WBANs, multi-biometric key creation, and dynamic metadata rebuilding. International Journal of Engineering Research & Science & Technology, 16(4).

[7] Langseth, P., Stapenhurst, R., & Pope, J. (1997). The role of a national integrity system in fighting corruption. Commonwealth Law Bulletin, 23(1-2), 499-528.

[8] Mohanarangan, V.D. (2020). Assessing Long-Term Serum Sample Viability for Cardiovascular Risk Prediction in Rheumatoid Arthritis. International Journal of Information Technology & Computer Engineering, 8(2), 2347–3657.

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[9] Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., &Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3.

[10] Koteswararao, D. (2020). Robust Software Testing for Distributed Systems Using Cloud Infrastructure, Automated Fault Injection, and XML Scenarios. International Journal of Information Technology & Computer Engineering, 8(2), ISSN 2347–3657.

[11] Vatsa, V., Sural, S., & Majumdar, A. K. (2007). A rule-based and game-theoretic approach to online credit card fraud detection. International Journal of Information Security and Privacy (IJISP), 1(3), 26-46.

[12] Rajeswaran, A. (2020). Big Data Analytics and Demand-Information Sharing in ECommerce Supply Chains: Mitigating Manufacturer Encroachment and Channel Conflict. International Journal of Applied Science Engineering and Management, 14(2), ISSN2454-9940

[13] Behdad, M., Barone, L., Bennamoun, M., & French, T. (2012). Nature-inspired techniques in the context of fraud detection. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42(6), 1273-1290.

[14] Alagarsundaram, P. (2020). Analyzing the covariance matrix approach for DDoS HTTP attack detection in cloud environments. International Journal of Information Technology & Computer Engineering, 8(1).

[15] Save, P., Tiwarekar, P., Jain, K. N., &Mahyavanshi, N. (2017). A novel idea for credit card fraud detection using decision tree. International Journal of Computer Applications, 161(13).

[16] Poovendran, A. (2020). Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. International Journal of Information technology & computer engineering, 8(2), I

[17] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. The economics of information security and privacy, 265-300.

[18] Sreekar, P. (2020). Cost-effective Cloud-Based Big Data Mining with K-means Clustering: An Analysis of Gaussian Data. International Journal of Engineering & Science Research, 10(1), 229-249.

[19] Ondiege, B., Clarke, M., & Mapp, G. (2017). Exploring a new security framework for remote patient monitoring devices. Computers, 6(1), 11.

[20] Karthikeyan, P. (2020). Real-Time Data Warehousing: Performance Insights of Semi-Stream Joins Using Mongodb. International Journal of Management Research & Review, 10(4), 38-49

[21] Sharma, M., & Jha, S. (2017). Digital data stealing from ATM using data skimmers: Challenge to the forensic examiner. Journal of Forensic Sciences & Criminal Investigation, 1(4).

[22] Mohan, R.S. (2020). Data-Driven Insights for Employee Retention: A Predictive Analytics Perspective. International Journal of Management Research & Review, 10(2), 44-59.

[23] Zulkurnain, A. U., Hamidy, A. K. B. K., Husain, A. B., &Chizari, H. (2015). Social engineering attack mitigation. Int. J. Math. Comput. Sci, 1(4), 188-198.

[24] Sitaraman, S. R. (2020). Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques. International Journal of Engineering Research and Science & Technology, 16(3), 9-22.

[25] Nagar, G. (2018). Leveraging Artificial Intelligence to Automate and Enhance Security Operations: Balancing Efficiency and Human Oversight. Valley International Journal Digital Library, 78-94.

[26] Panga, N. K. R. (2020). Leveraging heuristic sampling and ensemble learning for enhanced insurance big data classification. International Journal of Financial Management (IJFM), 9(1).

[27] Aisyah, N., Hidayat, R., Zulaikha, S., Rizki, A., Yusof, Z. B., Pertiwi, D., & Ismail, F. (2019). Artificial Intelligence in Cryptographic Protocols: Securing E-Commerce Transactions and Ensuring Data Integrity.

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[28] Gudivaka, R. L. (2020). Robotic Process Automation meets Cloud Computing: A Framework for Automated Scheduling in Social Robots. International Journal of Business and General Management (IJBGM), 8(4), 49-62.

[29] Behdad, M., Barone, L., Bennamoun, M., & French, T. (2012). Nature-inspired techniques in the context of fraud detection. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42(6), 1273-1290.

[30] Gudivaka, R. K. (2020). Robotic Process Automation Optimization in Cloud Computing Via Two-Tier MAC and LYAPUNOV Techniques. International Journal of Business and General Management (IJBGM), 9(5), 75-92.

[31] Mozzaquatro, B. A., Agostinho, C., Goncalves, D., Martins, J., & Jardim-Goncalves, R. (2018). An ontology-based cybersecurity framework for the internet of things. Sensors, 18(9), 3053.

[32] Deevi, D. P. (2020). Artificial neural network enhanced real-time simulation of electric traction systems incorporating electro-thermal inverter models and FEA. International Journal of Engineering and Science Research, 10(3), 36-48.

[33] Sharma, R., Pavlovic, V. I., & Huang, T. S. (2002). Toward multimodal human-computer interface. Proceedings of the IEEE, 86(5), 853-869.

[34] Allur, N. S. (2020). Enhanced performance management in mobile networks: A big data framework incorporating DBSCAN speed anomaly detection and CCR efficiency assessment. Journal of Current Science, 8(4).

[35] Skipper, H. D. (2000). Financial services integration worldwide: Promises and pitfalls. North American Actuarial Journal, 4(3), 71-108.

[36] Deevi, D. P. (2020). Real-time malware detection via adaptive gradient support vector regression combined with LSTM and hidden Markov models. Journal of Science and Technology, 5(4).

[37] Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. Data mining and knowledge discovery, 18, 30-55.

[38] Dondapati, K. (2020). Integrating neural networks and heuristic methods in test case prioritization: A machine learning perspective. International Journal of Engineering & Science Research, 10(3), 49–56.

[39] Leskovec, J., Krause, A., Guestrin, C., Faloutsos, C., VanBriesen, J., & Glance, N. (2007, August). Cost-effective outbreak detection in networks. In Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 420-429).

[40] Dondapati, K. (2020). Leveraging backpropagation neural networks and generative adversarial networks to enhance channel state information synthesis in millimeter-wave networks. International Journal of Modern Electronics and Communication Engineering, 8(3), 81-90

[41] Brodie, M. L. (1993). The promise of distributed computing and the challenges of legacy information systems. In Interoperable database systems (DS-5) (pp. 1-31). North-Holland.

[42] Gattupalli, K. (2020). Optimizing 3D printing materials for medical applications using AI, computational tools, and directed energy deposition. International Journal of Modern Electronics and Communication Engineering, 8(3).

[43] Brown, D. K. (2018). How to Marginalize Criminal Trials Without Pretrial Discovery. Virginia Public Law and Legal Theory Research Paper, (2018-24), 55.

[44] Allur, N. S. (2020). Big data-driven agricultural supply chain management: Trustworthy scheduling optimization with DSS and MILP techniques. Current Science & Humanities, 8(4), 1–16.

[45] Guo, X., Yin, Y., Dong, C., Yang, G., & Zhou, G. (2008, October). On the class imbalance problem. In 2008 Fourth international conference on natural computation (Vol. 4, pp. 192-201). IEEE.

[46] Narla, S., Valivarthi, D. T., & Peddi, S. (2020). Cloud computing with artificial intelligence techniques: GWO-DBN hybrid algorithms for enhanced disease prediction in healthcare systems. Current Science & Humanities, 8(1), 14–30.

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[47] Gudala, L., Shaik, M., Venkataramanan, S., & Sadhu, A. K. R. (2019). Leveraging artificial intelligence for enhanced threat detection, response, and anomaly identification in resource-constrained iot networks. Distributed Learning and Broad Applications in Scientific Research, 5, 23-54.

[48] Kethu, S. S. (2020). AI and IoT-driven CRM with cloud computing: Intelligent frameworks and empirical models for banking industry applications. International Journal of Modern Electronics and Communication Engineering (IJMECE), 8(1), 54.

[49] Jena, J. (2015). Next-Gen Firewalls Enhancing: Protection against Modern Cyber Threats. International Journal of Multidisciplinary and Scientific Emerging Research, 4(3), 2015-2019.

[50] Vasamsetty, C. (2020). Clinical decision support systems and advanced data mining techniques for cardiovascular care: Unveiling patterns and trends. International Journal of Modern Electronics and Communication Engineering, 8(2).

[51] Enemosah, A. (2019). Implementing DevOps Pipelines to Accelerate Software Deployment in Oil and Gas Operational Technology Environments. International Journal of Computer Applications Technology and Research, 8(12), 501-515.

[52] Kadiyala, B. (2020). Multi-swarm adaptive differential evolution and Gaussian walk group search optimization for secured IoT data sharing using supersingular elliptic curve isogeny cryptography,International Journal of Modern Electronics and Communication Engineering,8(3).

[53] Taylor, S. J., Anagnostou, A., Kiss, T., Terstyanszky, G., Kacsuk, P., Fantini, N., ... & Costes, J. (2018). Enabling cloud-based computational fluid dynamics with a platform-as-a-service solution. IEEE transactions on industrial informatics, 15(1), 85-94.

[54] Valivarthi, D. T. (2020). Blockchain-powered AI-based secure HRM data management: Machine learning-driven predictive control and sparse matrix decomposition techniques. International Journal of Modern Electronics and Communication Engineering.8(4)

[55] Shah, V., & Shukla, S. (2017). Data distribution into distributed systems, integration, and advancing machine learning. Revista Espanola de DocumentacionCientifica, 11(1), 83-99.

[56] Jadon, R. (2020). Improving AI-driven software solutions with memory-augmented neural networks, hierarchical multi-agent learning, and concept bottleneck models. International Journal of Information Technology and Computer Engineering, 8(2).

[57] L'heureux, A., Grolinger, K., Elyamany, H. F., &Capretz, M. A. (2017). Machine learning with big data: Challenges and approaches. Ieee Access, 5, 7776-7797.

[58] Boyapati, S. (2020). Assessing digital finance as a cloud path for income equality: Evidence from urban and rural economies. International Journal of Modern Electronics and Communication Engineering (IJMECE), 8(3).

[59] Leo, M., Sharma, S., &Maddulety, K. (2019). Machine learning in banking risk management: A literature review. Risks, 7(1), 29.

[60] Gaius Yallamelli, A. R. (2020). A cloud-based financial data modeling system using GBDT, ALBERT, and Firefly algorithm optimization for high-dimensional generative topographic mapping. International Journal of Modern Electronics and Communication Engineering8(4).

[61] Carvalho, D. V., Pereira, E. M., & Cardoso, J. S. (2019). Machine learning interpretability: A survey on methods and metrics. Electronics, 8(8), 832.

[62] Yalla, R. K. M. K., Yallamelli, A. R. G., &Mamidala, V. (2020). Comprehensive approach for mobile data security in cloud computing using RSA algorithm. Journal of Current Science & Humanities, 8(3).

[63] Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., &Vatrapu, R. (2019). Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. Journal of Management Information Systems, 36(1), 37-73.

Received: 2021-01-01
Accepted: 2021-01-15
Published Online: 2021-01-30
DOI: 10.70454/IJMRE.2021.10101

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

[64] Samudrala, V. K. (2020). AI-powered anomaly detection for cross-cloud secure data sharing in multi-cloud healthcare networks. Journal of Current Science & Humanities, 8(2), 11–22.

[65] Zhang, B., Qi, S., Monkam, P., Li, C., Yang, F., Yao, Y. D., & Qian, W. (2019). Ensemble learners of multiple deep CNNs for pulmonary nodules classification using CT images. IEEE Access, 7, 110358-110371.

[66] Ayyadurai, R. (2020). Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions. World Journal of Advanced Engineering Technology and Sciences, 1(1), 110–120.

[67] Lane, T., & Brodley, C. E. (2003). An empirical study of two approaches to sequence learning for anomaly detection. Machine learning, 51, 73-107.

[68] Chauhan, G. S., & Jadon, R. (2020). AI and ML-powered CAPTCHA and advanced graphical passwords: Integrating the DROP methodology, AES encryption, and neural network-based authentication for enhanced security. World Journal of Advanced Engineering Technology and Sciences, 1(1), 121–132.

[69] Zhang, D., Han, X., & Deng, C. (2018). Review on the research and practice of deep learning and reinforcement learning in smart grids. CSEE Journal of Power and Energy Systems, 4(3), 362-370.

[70] Narla, S. (2020). Transforming smart environments with multi-tier cloud sensing, big data, and 5G technology. International Journal of Computer Science Engineering Techniques, 5(1), 1-10.

[71] Omopariola, B. J., &Aboaba, V. (2019). Comparative analysis of financial models: Assessing efficiency, risk, and sustainability. Int J Comput Appl Technol Res, 8(5), 217-231.

[72] Alavilli, S. K. (2020). Predicting heart failure with explainable deep learning using advanced temporal convolutional networks. International Journal of Computer Science Engineering Techniques, 5(2).