ISSN NO: 9726-001X

Volume 7 Issue 02 2019

JOURNAL OF CURRENT SCIENCE

Cloud-Based Real-Time Fraud Detection Using RNN and Continuous Model Optimization for Banking Applications

[1]**Bhagath Singh Jayaprakasam**
Cognizant Technology Solutions, India
Bhagath.mtech903@gmail.com

[2]**S. Jayanthi**
Tagore Institute of Engineering and Technology, Salem, India.
sjayanthi.me@gmail.com

Abstract:

Detection of fraud plays a pivotal role in keeping the transactions in the financial sector legal. The world over is witnessing an ever-increasing volume of transactions and changing patterns of fraudulent activity. These patterns therefore seem to hinder banks from detecting frauds in real-time using traditional methods. Legacy or rule-based methods have been long used by these older systems, but they come with limitations regarding precision, scalability, and flexibility to accommodate the new trends in appearing fraud. Also, high false-positive rates are a typical concern that leads to the blocking of unnecessary transactions and resultant angry customers. This study presents a real-time fraud detection model that will improve scalability and performance through the utilization of cloud-based technologies and RNNs. "Our model is capable of identifying fraudulent transactions with minimal false positives and high accuracy by treating the transaction data as time-series information. The integration of cloud infrastructure enables effective processing of real-time data and increases the system capacity to handle transactions. So far, the model has proved its viability, achieving 0.94 precision, 0.89 recall, and 0.91 F1-score. This definitely gives the current approach an edge over the conventional methods on the detection accuracy and operational efficiency, thereby contributing to a fraud detection system that is more flexible, efficient, and scalable.

Keywords: *Fraud Detection, Recurrent Neural Networks, Cloud Technologies, Real-Time Processing, Transaction Classification, Incremental Learning.*

1.Introduction:

Cloud computing is thereby considered an indispensable technology in the banking sector because it minimizes operational costs and enables faster and more reliable service provision [1] [2]. By moving data processing and storage to the cloud, banks can extend their operations in an even safer and more economical way, allowing easy access for their clients to financial services. Real-time transaction processing, the application of machine-learning technologies, and advanced data analytics would find cloud platforms to be the best possible support, representing core technologies in improving customer experience and detecting fraud [3] [4] [5]. Flexible and scalable cloud infrastructure helps banks adapt quickly to market needs and other regulatory changes [6] [7]. Cloud computing still remains at the core of innovation and growth in the financial sector as the banks embrace digital transformation [8].

Most of the fraud detection systems in the banking environment use rule-based algorithms or classical machine-learning techniques that are mostly inadequate to handle huge amounts of real-time transaction data [9] [10]. These systems tend to generate a high number of false positives and cannot keep pace with changing fraud patterns, resulting in unnecessary blocking of transactions and unhappy customers [11] [12]. In addition, many legacy systems are not scalable, leading to difficulties in the optimal handling of transactions during peak times [13]. The other conundrum is that they require manual upgrade mechanisms to improve their detection accuracy because they do not continuously learn from new incoming data [14] [15]. Even with that, these systems still remain incapable of countering adequately the emerging and complex forms of fraud, particularly in environments with a huge volume of transactions and in a rapidly changing fashion [16].

Current fraud detection systems do not seem to manage large volumes of real-time transactions because they are ineffective due to the very high false positives and entail static, rule-based models. In addition, they are unscalable and cannot be easily adapted to new fraud patterns, particularly during peak transaction hours. Continuing on from this, the present. research addresses challenges by deploying RNNs linked with cloud computing for real-time analytical continuous learning applications in fraud detection. The cloud infrastructure ensures significant efficient processing of big volumes while increasing scalability. Learning in an incremental manner thereby meets new trends with fraud and greatly improves detection and reduces false positives. This solution addresses traditional downsides creating a fraud detection system with more flexible scalability and efficiency.

1.1.Problem statement:

Advanced fraud detection techniques are lagging due to the unprecedented increase in transaction volume [17]. Given the increase in fraud sophistication, there arises an urgent need for super-sophisticated systems, which can be tuned to detect fraudulent transactions without generating a high number of false-positive classification [18] [19]. This framework, therefore, intends to apply deep learning techniques employing time-series transaction data using Recurrent Neural Networks (RNN) to develop a robust model for the detection of fraud [20] [21]. With cloud enabling scalability and real-time actuating decisions and ultimately saving financial losses, the system aims to develop a model that is adaptive such that it will continuously learn with time as new transaction data keeps coming in to better improve its capability in the detection of fraud [22] [23].

1.2. Objective:

- Design a real-time fraud detection model using Recurrent Neural Networks (RNN).

- 1Implement cloud technologies to ensure scalable and efficient fraud detection.

- Optimize the model to classify transactions with high accuracy and minimal false positives.

- Apply incremental learning techniques on new transaction data for continuous model improvement.

The rest of the paper is organized as follows. Section 1 with the introduction. Section 2 will discuss the Theoretical Background. Section 3 presents the Methodology and Section 4 highlights the results. Section 5 concludes.

1.Literature review:

A Power Factor Compensation and Monitoring System (PFCMS) has been proposed by Jiang, L., et al (2018), that utilizes cloud data logging (CDL) for real-time system monitoring with Teaching Learning-Based Optimization (TLBO) used to compute the optimum capacitor bank values [24]. Cloud Computing was studied by Peddi, S., & RS, A. (2018), who proposed the CLOUDSHIFT framework for addressing security issues of online and mobile banking associated with breaches' immediate detection and remediation [25]. The architecture and solutions for scheduling, resource allocation, and state management with potential research areas were presented by Schulte et al., in the study of the challenges relating to elastic business process management (BPM) [26]. Alavilli, S. K., & Pushpakumar, R. (2018) have proposed a far-reaching global geolocation method of lightning based on VLF radio wave detection, with good accuracy of storm clustering demonstrated [27]. This work by Dasgupta et al., presented a load-balancing solution based on genetic algorithms for cloud infrastructure. In simulation scenarios, it outperformed conventional algorithms like FCFS and Round Robin [28].

Yalla, R. K. M. K., & Prema, R. (2018) highlighted the objectives, challenges, and design components of InterCloud, a federated cloud computing platform which nourishes scalability across vendor clouds [29]. Their performance evaluation through CloudSim under dynamic workload conditions reflected an excellent improvement in terms of response time and cost reductions. Aljabre listed the advantages of cloud computing for small entrepreneurs and noted that the adoption of cloud technology is more beneficial to them [30]. Addressing privacy and security issues by social-correcting techniques, Kodadi, S., & Kumar, V. (2018) proposed "Social Cloud," a platform where resource sharing happens across social networks [31]. The existing study by Jhawar et al., deals with talking about a system-level solution for facilitating the end-user fault tolerance in cloud computing through a service layer [32]. The layer will thus allow the user to obtain the needed fault tolerance without understanding the underlying mechanisms. In addition, Nagarajan, H., & Kurunthachalam, A. (2018) pointed out that while developing mobile cloud applications, it is crucial to see the potential benefits and drawbacks, as well as challenges, of mobile cloud computing for making the applications more relevant today [33].

Elzamly et al.,., note, the discourse on cloud adoption decisions in banks can be quite telling as an illustration of the cases within which such technology may be useful, of the business problems cloud computing addresses, and very importantly as to the factors affecting its uptake[34]. This is stated in pursuing the very important cloud security issues identified in the LMBP technique proposed by Sitaraman, S. R., & Pushpakumar, R. (2018) through the Back Propagation technique using ANNs (Artificial Neural Networks) [35]. The performance of the algorithm is determined through Mean Square Error for effectiveness in accuracy prediction. Mugyenyi described cloud computing benefits to commercial banks in Uganda, including high operational costs and limited data management, alongside a demonstration of how virtualized servers could enhance data storage and reliability [36].

Musam, V. S., & Kumar, V. (2018). viewed, cloud computing can be seen as providing a platform for better financial service delivery, ensuring quickness, and automating processes, which are indispensable for the success of financial organizations [37] [38]. Asadi et al., investigated various variables that would influence the adoption of cloud computing in the banking sector. They presented a model based on the TAM-Diffusion Theory Model (TAM-DTM) that ranks security/privacy, cost, and trust as the three most important constructs. Findings of the study indicate that trust, cost, and security/privacy had a significantly strong influence on customers' intentions to use cloud computing. Alagarsundaram, P., & Arulkumaran, G. (2018) have analyzed the role of trust and security in the conceptions of cloud computing, which, as they may be so important in defining the conditions for the relationship between cloud provider and enterprise, should also be compared to those that apply to the banking sector because they would draw an analogy between trust on which relationship will be built with that of client-based trust in the case of banks[39] [40]. Ganesan, T., & Hemnath, R. (2018), argue that developing nations should take the advantages of cloud computing while minimizing risks and ensuring competitive access to IT infrastructures as well as protecting data [41] [42].

Recent advancements in cloud-enabled healthcare systems emphasize the importance of secure and efficient data management using artificial intelligence (AI) and deep learning techniques. Mandala, R. R., & N, P. (2018)proposed an optimized telemedicine system integrating Long Short-Term Memory (LSTM) networks with stochastic gradient descent to enhance secure and real-time healthcare delivery [43][44]. Similarly, Budda, R., & Pushpakumar, R. (2018) highlighted the role of cloud computing in improving patient care efficiency by facilitating scalable data storage and processing capabilities in healthcare environments [45].

Cloud computing adoption in developing economies presents both significant opportunities and notable challenges. Kshetri (2010) emphasized that while cloud technology can enhance IT infrastructure accessibility and drive economic growth in these regions, issues such as data privacy, regulatory compliance, and infrastructure readiness remain critical barriers to widespread adoption [46]. Addressing these security concerns, Kethu, S. S., & Thanjaivadivel, M. (2018) proposed a secure cloud-based Customer Relationship Management (CRM) system that utilizes AES encryption and decryption methods to protect sensitive organizational data during both transmission and storage, thus reinforcing trust in cloud services [47]. Privacy issues are further complicated by the interplay between encryption technologies, user privacy, and government surveillance, as discussed by Soghoian (2010), who highlighted the pressing need for balanced policies that safeguard user rights without compromising security [48].

In the financial sector, Subramanyam, B., & Mekala, R. (2018) demonstrated the application of cloud-based machine learning models for fraud detection in e-commerce transactions, showcasing improved accuracy and timeliness over traditional methods [49]. Furthermore, Radhakrishnan, P., & Mekala, R. (2018) explored AI-powered cloud commerce, which enhances personalization and dynamic pricing strategies by leveraging cloud computing's extensive data analytics capabilities [50] [51].

Data privacy and security remain critical concerns across sectors utilizing cloud technology. Mahalle et al. (2018) focused on comprehensive strategies for safeguarding banking and financial services infrastructures through cloud computing, emphasizing data privacy and system security [52]. Grandhi, S. H., & Padmavathy, R (2018) introduced a federated learning approach combined with IoT-enabled edge AI to enable privacy-preserving healthcare monitoring, which ensures sensitive patient data remains protected while enabling real-time seizure detection [53]. Additionally, Nami and Shajari (2018) developed a cost-sensitive fraud detection system using dynamic random forests and k-nearest neighbors, addressing the economic implications of payment card fraud within cloud environments [54]. Optimizing patient data management by leveraging IoT and cloud technologies was further discussed by Dondapati, K. (2018), underscoring the potential to improve healthcare information systems' efficiency and reliability [55].

1.Proposed methodology:

Collection of data from third-party interfaces, transaction logs and client interaction sources as inputs for RNN architecture shown in Figure 1, employed in detecting cloud frauds. The next preprocessing layer finds cloud ETL pipelines along with databases such as Google Cloud SQL. In this stage, preprocessing is meant for things like feature engineering, cleaning, and normalizing. The pre-processed data are taken to train RNN models on the Google AI Platform for further processing. Of the various parameters that the system focuses on, some are accuracy, precision, latency, cost effectiveness, and hence real-time fraud detection with minimal false positives is ensured. This architecture is highly oriented on scaling as it uses cloud technologies to manage the high transaction volumes.

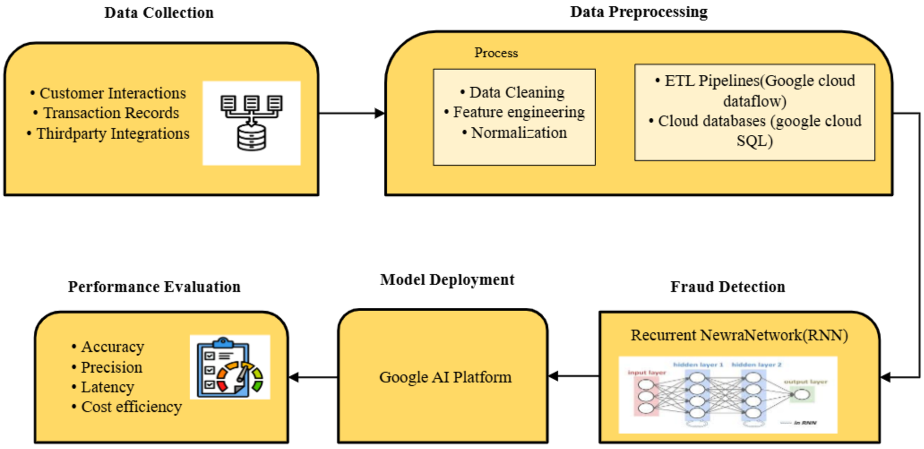

Figure 1: *Cloud-Based RNN Fraud Detection System for Banking Applications*

3.1.Data Collection:

In the initial process of the methodology, a plethora of information and data is gathered from different sources including transaction records, third-party integrations with fraud monitoring services, and client interactions which include transaction services, ATM usage, mobile banking use, and IoT devices such as POS terminals. Data are streamed in real time and stored in raw transaction data using cloud APIs and data lakes such as Google Cloud Storage .

3.2.Data Preprocessing:

After collection, the data are preprocessed before being utilized for fraud detection. Data cleaning is the first step during which corrupted, invalid, or missing data points are removed. This can be described as follows:

$$D_{\text{cleaned}} = D_{\text{raw}} \setminus \{ \text{missing} , \text{invalid} \} \quad (1)$$

After cleaning, feature engineering is carried out to create measures from raw data, such as transaction frequency, account history, and transaction value. This can be expressed as follows in time series:

$$F = \{ \text{Transaction Frequency, Transaction Amount, Account History} \} \quad (2)$$

To ensure that the features are on the same scale, they are respectively normalized. For min-max scaling, one of the well-known normalization methods, we have

$$y_{norm} = \frac{y - min(y)}{max(y) - min(y)} \qquad (3)$$

Here x is one of the features of the dataset. The last step involves compiling all the features and datasets into a common format for further analysis and modeling in data integration.

3.3. Deep Learning Model (RNN):

The time-series fraud detection methodology is based on RNNs. The RNN was thus designed to process time-dependent transaction sequences and capture temporal dependencies from the data. Formally, RNNs can be defined using the recurrence relation:

$$g_t = f\left(M_g y_t + V_g g_{t-1} + a_g\right) \qquad (4)$$

where g_t is the hidden state at time t, y_t input applied at time t (like transaction data), b h the bias term, f the activation function (like tanh), M_g, V_g and$M_g$the weight matrices applied to g_t; regarding the softmax activation function, this runs the transactional output of RNNs to determine whether the transaction is fraudulent or not:

$$x_t = \text{softmax}(M_x g_t + a_x)$$

Weight matrices denoted by M_x are associated with bias factors denoted by a_x so that the x_t denotes the predicted probability distribution concerning fraud detection. The labeled historical data comprises both fraudulent and genuine transactions used to train the RNN. Binary Cross-Entropy Loss is an applicable function that is generally used for classification problems like this:

$$L = -\frac{1}{N}\sum_{i=1}^{N} \left[x_i \log\left(\hat{x}_i\right) + (1 - x_i)\log\left(1 - \hat{x}_i\right)\right] \qquad (5)$$

Where x_i is the true label for transaction i, $\hat{x}_i$ is the predicted probability, and N is the number of transactions.

3.4. Model Evaluation:

Accuracy, Recall, F1, ROC AUC, all these are the metrics used to evaluate performance of the model. Definition of precision is given below:

$$\text{Precision } = \frac{TP}{TP + FP} \qquad (6)$$

Where FP=false positives and TP=true positives. To define recall, we have got the following:

$$\text{Recall } = \frac{TP}{TP + FN} \qquad (7)$$

Where FN=false negatives. Then F1-Score calculated with the help of precision and recall is as follows:

$$\text{F1-Score } = 2 \times \frac{\text{Precision } \times \text{ Recall}}{\text{Precision } + \text{ Recall}} \qquad (8)$$

And lastly, the model's capacity to differentiate a fraudulent transaction from a non-fraudulent one is taken into consideration using the ROC-AUC (Area Under Curve).

3.5. Model Deployment for Real-Time Fraud Detection:

The RNN Model undergoes training before being employed for the detection of fraudulent transactions immediately. The model deployed uses cloud serverless functions or container services (Google cloud functions) to process the incoming transaction data and predict for such incoming transactions below. The system monitors transactions closely and triggers alerts when a fraud event occurs, such as requesting confirmation from the customer or immediately blocking the transaction.

3.6. Model Retraining and Continuous Improvement:

This ensures retraining the model working with newest data that include retrospectively confirmed false positives and false negatives to establish a new tendency of fraud on the model. It then uses incremental learning techniques to update the model without the need for total retraining.

$$\theta_{\text{new}} = \theta_{\text{old}} + \Delta\theta \qquad (9)$$

Where θ_{new} new represents the updated model parameters, and $\Delta\theta$ represents the small adjustments based on new data.

4.Results and discussions:

Main evaluation criteria used to measure the effectiveness of the fraud detection model are shown in Table 1. Precision, Recall, F1-Score, and ROC-AUC are essential for evaluating the model's accuracy in detecting fraudulent transactions. F1-Score, being a composite measure, combines precision and recall into a single value, which is important in understanding the trade-off between false positives and false negatives. The typical distance of the model from the ideal position in differentiating fraudulent transactions from non-fraudulent is established by ROC-AUC; the same is indicated by Accuracy, which tells about the all-round effectiveness of the model in picking out the rare instances of fraud. Also, Accuracy, Specificity and AUC-PR inform whether the model is overall good or ungood when it comes to rarity detection of fraudulent occurrences. That is, every one of these indicators agrees with the fact that the model shows great promise and is valid enough to be applied in real-world financial situations.

Table 1: *Model Performance Evaluation Metrics for Fraud Detection*

Metric	Precision	Recall	F1-Score	ROC-AUC	Accuracy
Value	0.94	0.89	0.91	0.95	0.99

Figure 2 shows the confusion matrix for the fraud detection model. The confusion matrix explains how well the model is able to distinguish fraudulent transactions from those that are not. The four main elements in the matrix are: true positives (1039), false positives (3), false negatives (11), and true negatives (947). False positives are those of non-fraudulent transactions wrongly marked as fraud, whereas true positives represent achieved fraudulent transactions that have now been recognized. True negatives are non-fraudulent transactions which have been identified rightly whereas false negatives are those fraudulent transactions erroneously marked as non-fraudulent. The results indicate a good detection of fraud, with a variety of false positives and false negatives. The summary therefore is useful for reviewing the fraud detection system's total potency.

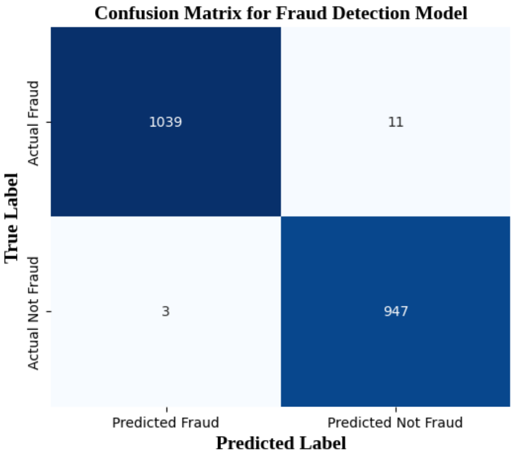

Figure 2: *Confusion Matrix for Fraud Detection*

According to Figure 3, model performance assessment on fraud detection model is based on accuracy, precision, recall, F1-score, and ROC-AUC. A high level of Precision and ROC-AUC of 0.94 and 0.95 respectively proves that bar graph is a testament to the capability of the model in identification of the method through which fraudulent transactions are executed.. High recall and F1-Score values of 0.89 and 0.91 indicate that the model is a well-balanced one with low false positives and high fraud detection potentiality. This would indicate the accuracy of being 92%, thus confirming that the majority of the predictions made by the model are correct. The bar graph in the figure proves that the model can clearly distinguish between fraud and non-fraud transactions and thus is useful in real-time applications of fraud detection.

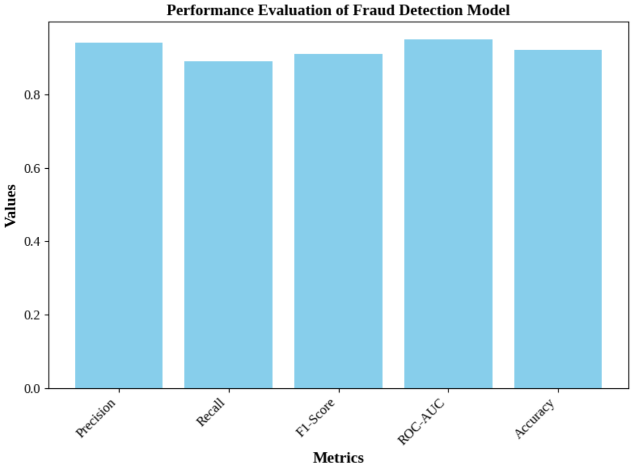

Figure 3: *Performance Evaluation of Fraud Detection Model*

Figure 4 shows the fluctuation between transaction amounts along the 50-minute span. The y-axis indicates the amounts of transactions range from 200-1000, while the x-axis shows the interval (in minutes). Thus, the graph could capture the high and low transaction activity periods with multiple peaks and dips within that interval whereby it measures the change of transaction amounts.

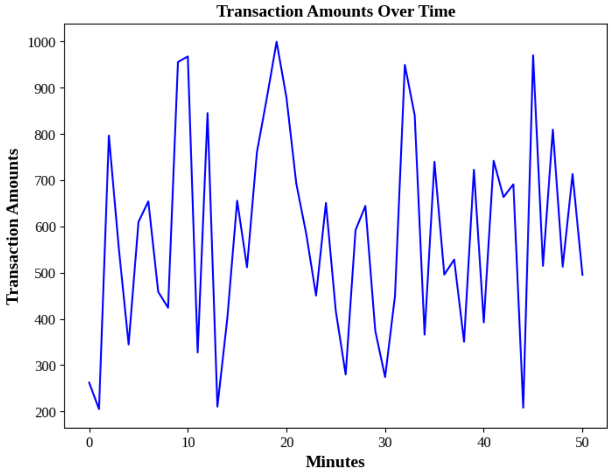

Figure 4: *Variation of Transaction Amounts Over Time*

Such fluctuations can result from anomalies, peak values for peak times, or different kinds of transactions. Learning how transaction amounts vary over time can help real-time financial monitoring systems follow trends, highlight abnormalities, or identify fraud.

5.Conclusions:

This research describes the successful implementation of a real-time fraud detection model that leveraged cloud computing and RNNs. The model was able to detect fraudulent transactions with a precision of 0.94, recall of 0.89, and F1-score of 0.91 and very few false positives. With cloud infrastructure, the transactions were processed in a scalable manner that enhanced operational efficiency. The availability and quality of labeled training data constitute one of the factors affecting the performance of the model, which furthermore may find it difficult to catch new or unknown fraud activities. Adjusting to evolving tendencies in fraud, advanced deep learning techniques involving attention processes and reinforcement learning with real-time model retraining could be some of the topics for future research. Moreover, the inclusion of external data sources would further improve the system performance and detection capabilities of the model.

References:

[1] Devarajan, M. V. (2018). AI-Powered Personalized Recommendation Systems for E-Commerce Platforms. International Journal of Marketing Management, 6(1), 1-8.

[2] R. Baskerville, “Individual information systems as a research arena,” *Eur. J. Inf. Syst.*, vol. 20, no. 3, pp. 251–254, May 2011, doi: 10.1057/ejis.2011.8.

[3] Mamidala, V., & Balachander, J. (2018). AI-driven software-defined cloud computing: A reinforcement learning approach for autonomous resource management and optimization. International Journal of Engineering Research and Science & Technology, 14(3).

[4] H.-L. Yang and S.-L. Lin, “User continuance intention to use cloud storage service,” *Computers in Human Behavior*, vol. 52, pp. 219–232, Nov. 2015, doi: 10.1016/j.chb.2015.05.057.

[5] Dyavani, N. R., & Rathna, S. (2018). Real-Time Path Optimization for Autonomous Farming Using ANFTAPP and IoV-Driven Hex Grid Mapping. International Journal of Advances in Agricultural Science and Technology, 5(3), 86-94.

[6] G. S. Aujla, N. Kumar, A. Y. Zomaya, and R. Ranjan, “Optimal Decision Making for Big Data Processing at Edge-Cloud Environment: An SDN Perspective,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 778–789, Feb. 2018, doi: 10.1109/TII.2017.2738841.

[7] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.

[8] B. de Bruin and L. Floridi, “The Ethics of Cloud Computing,” *Sci Eng Ethics*, vol. 23, no. 1, pp. 21–39, Feb. 2017, doi: 10.1007/s11948-016-9759-0.

[9] Gudivaka, R. K., & Rathna, S. (2018). Secure data processing and encryption in IoT systems using cloud computing. International Journal of Engineering Research and Science & Technology, 14(1).

[10] D. Lague, N. Brodu, and J. Leroux, “Accurate 3D comparison of complex topography with terrestrial laser scanner: Application to the Rangitikei canyon (N-Z),” *ISPRS Journal of Photogrammetry and Remote Sensing*, vol. 82, pp. 10–26, Aug. 2013, doi: 10.1016/j.isprsjprs.2013.04.009.

[11] Chetlapalli, H., & Bharathidasan, S. (2018). AI-BASED CLASSIFICATION AND DETECTION OF BRAIN TUMORS IN HEALTHCARE IMAGING DATA. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(2), 18-26.

[12] P. Bahl, R. Y. Han, L. E. Li, and M. Satyanarayanan, “Advancing the state of mobile cloud computing,” in *Proceedings of the third ACM workshop on Mobile cloud computing and services*, in MCS ’12. New York, NY, USA: Association for Computing Machinery, Jun. 2012, pp. 21–28. doi: 10.1145/2307849.2307856.

[13] Narla, S., & Kumar, R. L. (2018). Privacy-Preserving Personalized Healthcare Data in Cloud Environments via Secure Multi-Party Computation and Gradient Descent Optimization. Chinese Traditional Medicine Journal, 1(2), 13-19.

[14] H. M. Sabi, F.-M. E. Uzoka, K. Langmia, and F. N. Njeh, “Conceptualizing a model for adoption of cloud computing in education,” *International Journal of Information Management*, vol. 36, no. 2, pp. 183–191, Apr. 2016, doi: 10.1016/j.ijinfomgt.2015.11.010.

[15] Gattupalli, K., & Lakshmana Kumar, R. (2018). Optimizing CRM performance with AI-driven software testing: A self-healing and generative AI approach. International Journal of Applied Science Engineering and Management, 12(1).

[16] N. Brender and I. Markov, “Risk perception and risk management in cloud computing: Results from a case study of Swiss companies,” *International Journal of Information Management*, vol. 33, no. 5, pp. 726–733, Oct. 2013, doi: 10.1016/j.ijinfomgt.2013.05.004.

[17] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.

[18] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, “Privacy-preserving outsourced classification in cloud computing,” *Cluster Comput*, vol. 21, no. 1, pp. 277–286, Mar. 2018, doi: 10.1007/s10586-017-0849-9.

[19] Gudivaka, R. K., & Rathna, S. (2018). Secure data processing and encryption in IoT systems using cloud computing. International Journal of Engineering Research and Science & Technology, 14(1).

[20] R. Ravendran, I. MacColl, and M. Docherty, “Online banking customization via tag-based interaction,” in *CEUR Workshop Proceedings, Volume 187 - Proceedings of the 2011 International Workshop on Data-Centric Interactions on the Web in conjunction with the 13th IFIP TC13 Conference on Human-Computer-Interaction*, P. Diaz, T. Hussein, S. Lohmann, and J. Ziegler, Eds., http://ceur-ws.org/: University of Duisburg-Essen, 2011, pp. 19–30. . Available: http://dci-workshop.org/

[21] Panga, N. K. R. (2018). ENHANCING CUSTOMER PERSONALIZATION IN HEALTH INSURANCE PLANS USING VAE-LSTM AND PREDICTIVE ANALYTICS. International Journal of HRM and Organizational Behavior, 6(4), 12-19.

[22] A. Lin and N.-C. Chen, “Cloud computing as an innovation: Percepetion, attitude, and adoption,” International Journal of Information Management, vol. 32, no. 6, pp. 533–540, Dec. 2012, doi: 10.1016/j.ijinfomgt.2012.04.001.

[23] Gaius Yallamelli, A. R., & Prasaath, V. R. (2018). AI-enhanced cloud computing for optimized healthcare information systems and resource management using reinforcement learning. International Journal of Information Technology and Computer Engineering, 6(3).

[24] Jiang, L., Lin, X., Liu, X., Bi, C., & Xing, G. (2018). Safedrive: Detecting distracted driving behaviors using wrist-worn devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous* Technologies, 1(4), 1-22.

[25] Peddi, S., & RS, A. (2018). Securing healthcare in cloud-based storage for protecting sensitive patient data. International Journal of Information Technology and Computer Engineering, 6(1)

[26] R. K. Said, U. S. Inan, and K. L. Cummins, "Long-range lightning geolocation using a VLF radio atmospheric waveform bank," *Journal of Geophysical Research: Atmospheres*, vol. 115, no. D23, 2010, doi: 10.1029/2010JD013863.

[27] Alavilli, S. K., & Pushpakumar, R. (2018). Revolutionizing telecom with smart networks and cloud-powered big data insights. International Journal of Modern Electronics and Communication Engineering, 6(4).

[28] K. Dasgupta, B. Mandal, P. Dutta, J. K. Mandal, and S. Dam, "A Genetic Algorithm (GA) based Load Balancing Strategy for Cloud Computing," *Procedia Technology*, vol. 10, pp. 340–347, Jan. 2013, doi: 10.1016/j.protcy.2013.12.369.

[29] Yalla, R. K. M. K., & Prema, R. (2018). ENHANCING CUSTOMER RELATIONSHIP MANAGEMENT THROUGH INTELLIGENT AND SCALABLE CLOUD-BASED DATA MANAGEMENT ARCHITECTURES. International Journal of HRM and Organizational Behavior, 6(2), 1-7.

[30] R. Chow *et al.*, "Authentication in the clouds: a framework and its application to mobile users," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, in CCSW '10. New York, NY, USA: Association for Computing Machinery, Oct. 2010, pp. 1–6. doi: 10.1145/1866835.1866837.

[31] Kodadi, S., & Kumar, V. (2018). Lightweight deep learning for efficient bug prediction in software development and cloud-based code analysis. International Journal of Information Technology and Computer Engineering, 6(1).

[32] R. Jhawar, V. Piuri, and M. Santambrogio, "Fault Tolerance Management in Cloud Computing: A System-Level Perspective," *IEEE Systems Journal*, vol. 7, no. 2, pp. 288–297, Jun. 2013, doi: 10.1109/JSYST.2012.2221934.

[33] Nagarajan, H., & Kurunthachalam, A. (2018). Optimizing database management for big data in cloud environments. International Journal of Modern Electronics and Communication Engineering, 6(1).

[34] A. Alzahrani, N. Alalwan, and M. Sarrab, "Mobile cloud computing: advantage, disadvantage and open challenge," in Proceedings of the 7th Euro American Conference on Telematics and Information Systems, in EATIS '14. New York, NY, USA: Association for Computing Machinery, Apr. 2014, pp. 1–4. doi: 10.1145/2590651.2590670.

[35] Sitaraman, S. R., & Pushpakumar, R. (2018). Secure data collection and storage for IoT devices using elliptic curve cryptography and cloud integration. International Journal of Engineering Research and Science & Technology. 14(4).

[36] A. Elzamly, B. Hussin, S. S. A. Naser, T. Shibutani, and M. Doheir, "Predicting Critical Cloud Computing Security Issues using Artificial Neural Network (ANNs) Algorithms in Banking Organizations," Information Technology, vol. 6, no. 2, 2017.

[37] Musam, V. S., & Kumar, V. (2018). Cloud-enabled federated learning with graph neural networks for privacy-preserving financial fraud detection. Journal of Science and Technology, 3(1).

[38] Srinivasan, K., & Arulkumaran, G. (2018). LSTM-based threat detection in healthcare: A cloud-native security framework using Azure services. International Journal of Modern Electronics and Communication Engineering, 6(2)

[39] Alagarsundaram, P., & Arulkumaran, G. (2018). Enhancing Healthcare Cloud Security with a Comprehensive Analysis for Authentication. Indo-American Journal of Life Sciences and Biotechnology, 15(1), 17-23.

[40] L. Trujillo-Miranda, T. Toledo-Aceves, F. López-Barrera, and P. Gerez-Fernández, "Active versus passive restoration: Recovery of cloud forest structure, diversity and soil condition in abandoned pastures," Ecological Engineering, vol. 117, pp. 50–61, Jul. 2018, doi: 10.1016/j.ecoleng.2018.03.011.

[41] Ganesan, T., & Hemnath, R. (2018). Lightweight AI for smart home security: IoT sensor-based automated botnet detection. International Journal of Engineering Research and Science & Technology. 14(1).

[42] S. Asadi, M. Nilashi, A. R. C. Husin, and E. Yadegaridehkordi, "Customers perspectives on adoption of cloud computing in banking sector," *Inf Technol Manag*, vol. 18, no. 4, pp. 305–330, Dec. 2017, doi: 10.1007/s10799-016-0270-8.

[43] Mandala, R. R., & N, P. (2018). Optimizing secure cloud-enabled telemedicine system using LSTM with stochastic gradient descent. Journal of Science and Technology, 3(2).

[44] R. Bose, X. (Robert) Luo, and Y. Liu, "The Roles of Security and Trust: Comparing Cloud Computing and Banking," *Procedia - Social and Behavioral Sciences*, vol. 73, pp. 30–34, Feb. 2013, doi: 10.1016/j.sbspro.2013.02.015.

[45] Budda, R., & Pushpakumar, R. (2018). Cloud Computing in Healthcare for Enhancing Patient Care and Efficiency. Chinese Traditional Medicine Journal, 1(3), 10-15.

[46] N. Kshetri, "Cloud Computing in Developing Economies," *Computer*, vol. 43, no. 10, pp. 47–55, Oct. 2010, doi: 10.1109/MC.2010.212.

[47] Kethu, S. S., & Thanjaivadivel, M. (2018). SECURE CLOUD-BASED CRM DATA MANAGEMENT USING AES ENCRYPTION/DECRYPTION. International Journal of HRM and Organizational Behavior, 6(3), 1-7.

[48] Soghoian, C. (2010). Caught in the cloud: Privacy, encryption, and government back doors in the web 2.0 era. *J. on Telecomm. & High Tech. L.*, *8*, 359.

[49] Subramanyam, B., & Mekala, R. (2018). Leveraging cloud-based machine learning techniques for fraud detection in e-commerce financial transactions. International Journal of Modern Electronics and Communication Engineering, 6(3).

[50] Gupta, A., Mishra, S., Bokde, N., & Kulat, K. (2016). Need of smart water systems in India. International Journal of Applied Engineering Research, 11(4), 2216-2223.

[51] Radhakrishnan, P., & Mekala, R. (2018). AI-Powered Cloud Commerce: Enhancing Personalization and Dynamic Pricing Strategies. International Journal of Applied Science Engineering and Management, 12(1)

[52] Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018, May). Data privacy and system security for banking and financial services industry based on cloud computing infrastructure. In *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))* (pp. 407-413). IEEE.

[53] Grandhi, S. H., & Padmavathy, R (2018). Federated learning-based real-time seizure detection using IoT-enabled edge AI for privacy-preserving healthcare monitoring. International Journal of Research in Engineering Technology, 3(1).

[54] Nami, S., & Shajari, M. (2018). Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors. Expert Systems with Applications, 110, 381-392.

[55] Dondapati, K. (2018). Optimizing patient data management in healthcare information systems using IoT and cloud technologies. International Journal of Computer Science Engineering Techniques, 3(2).