

Research Article

DOI: <http://dx.doi.org/10.22192/ijamr.2018.05.06.011>

Leveraging Cloud Computing for Fraud Detection and Risk Management in Financial Services

¹**Yashwant Kumar Kolli**

Cognizant Technology Solutions US Corp,
College Station, Texas, USA
yashkolli04@gmail.com

²**Karthick.M**

SNS College of Technology, Coimbatore, India.
magukarthik@gmail.com

Abstract

Keywords

Fraud Detection, Cloud Computing, Risk Management, Long Short-Term Memory, Transaction Data, Data Storage, Scalability, Fraud Tactics

With an increase in the number as well as the complexity of digital transactions, the challenges posed on traditional fraud detection systems increase rapidly. One of the best counter-approaches is to provide the latest technologies, such as cloud computing, to facilitate fraud detection and risk management for the financial services setting. The method has proven scalable and effective. The very latest machine-learning technology puts into operation the use of long Short-Term Memory networks together with cloud technology for the accurate and constant monitoring of transaction data for fraud detection by financial institutions. Cloud computing enhances fraud detection in that it offers more data storage capacity for data processing and easier integration with data sources to expedite intervention investigations in risk mitigation. Added to the scalability and high availability afforded by the cloud, a fraud detection system would thus adjust and keep pace with changes in failure detection learning and model updating to counter differentiating fraud tactics. Moreover, with the enhanced fraud detection accuracy, this method would optimize risk management by allowing financial services to protect sensitive data and clients' confidence amid a fast-evolving digital landscape.

1. INTRODUCTION

While there has been a rapid surge in transactions over the digital platform, sadly, it has also given rise to the fraudulent and other financial crime [1]. The traditional detection mechanisms prove inadequate in front of the most advance and fasted fraudulent activities[2]. Hence, most financial institutions started heading toward the cloud. Cloud computing technologies provide scalability, [3]computational power, and real-time processing that can handle

massive volumes of data[4]. Thus, these advanced machine learning algorithms on the cloud shall help in real-time detection of the anomalies and will allow the system to act immediately on risk mitigation[5]. In addition to offering more accurate fraud detection systems with swift processing, another advantage of this paradigm is its continual learning and model updating[6]. Furthermore, completing all seamless integrations with the data sources within high availability and compliance is a factor of consideration for cloud solutions.[7] Therefore, these become rather

important in the modernization of financial fraud management from its original infrastructure. Besides enhancing fraud detection, cloud computing importantly supports risk management in financial services[8]. Cloud platforms enable institutions to perform advanced analytics, risk scoring, and automate decision-making with greater accuracy and speed through centralized secure and scalable data storage and processing. They provide infrastructure for proactively detecting and swiftly responding to high-risk activities: [9]specifically, real-time dashboards, AI model deployment pipelines, and data lakes. And cloud environments govern a secure ecosystem for departments to share data with their external regulators and track that data across cloud consumers.[10] Such integrated and cloud-supported risk management reduces the economic blow while assuring customers those institutions will detect, respond, and prevent fraud in a rapidly changing threat environment.[11]

1.1 Problem statement

Increasing domains of financial services in the digital world have enhanced the volume and the velocity of credit card transactions to an extent that conventional fraud detection systems feel overwhelmed in detecting and responding toward fraudulent activities in real time. [12]Rule-based systems and usual machine learning models seldom cope with the complex, ever-evolving patterns of fraudulent behavior, especially when these systems have been built on aged or even more static datasets. [13]Such systems also tend to generate many false positives, thus inconveniencing genuine customers, yet allowing masterful schemes of fraud to evade detection. In this way, not only are huge financial losses inflicted on the institutions, but they also lead to loss of trust from the customer and regulatory compliance[14]

In addition to accuracy, [15]another factor affecting the performance of the old generations of fraud detection systems is scalability, and this tussle yet again strikes against the walls keeping these systems inefficient. With the mushrooming of transaction data, on-premises setups confront a hard time maintaining real-time analytics along with dynamic risk assessment [16]. On top of it, financial institutions are, in fact, looking at a dual challenge, taking into account massive data stream processing and committing to high data security and privacy standards. Unless a flexible and high-performing solution exists, such as a cloud platform with intelligent models against the ever-evolving fraud landscape, timely deployment of

countermeasures for ensuring high-level financial security will become increasingly difficult

1.2 Objective

- Improving the Accuracy of Fraud Detection: Building an efficient fraud detection system on LSTM networks in a cloud-computing platform will allow real-time monitoring of transactions with much higher detection accuracy than conventional methods.
- Ensure Scalability and Flexibility: Using cloud infrastructure scales such that the fraud detection system can work on massive transaction data and adapt excellently to increased transaction loads.
- Enhancing Data Processing and Real-Time Risk Management: Cloud technology with machine learning models to ensure that data processing is done rapidly, with the immediate risk management application of the LSTM, allowing financial institutions to detect and act on fraud instantaneously.
- Maximization of Feature Selection and Model Performance: This has included advanced techniques such as Firefly Optimization for feature selection, for increased efficiency in the model with reduced dimensionality and improved fraud detection performance.
- Help Data Protection and Compliance: Allow cloud service compliance with standards for data security such as PCI DSS, GDPR, and HIPAA to provide the respective privacy and confidentiality of the highly sensitive financial information with permitting easy integration and storage.

2. LITERATURE SURVEY

In recent times, the rapid advancement of digital financial ecosystems has raised the volume of transactions to an unprecedented level, thus compounding the difficulty in detecting fraudulent activities[17]. At this point, traditional rule-based systems with the existing statistical approaches can no longer measure up to the actual capability needed in real-time analysis of changing patterns of fraud. Foundation work on the application of statistical models in anomaly detection for financial transactions dates to early studies such as Bolton and Hand but both fail to scale and adapt to modern threats[18]. With the emergence of big data and cloud computing, machine learning has been linked to scalable infrastructures to increase detection accuracy and speed. For example, Phua et al. studied the various

ways of applying data mining to fraud detection; they also stressed the limitations of static models when employed in a dynamic environment [19].

Cloud computing has changed dramatically regarding fraud detection, offering elastic computing resources, high availability, and quick deployment features. According to cloud-based infrastructures facilitate the real-time collection of massive datasets of transactions, processing, and analysis, which are critical for the training of fraud detection models. Most cloud platforms, such as AWS, Azure, and Google Cloud, already integrated with tools like TensorFlow, Spark, and Hadoop, enable distributed model training and inference at scale. These capabilities allow financial institutions to continuously monitor transaction streams and quickly retrain models based on the latest fraud patterns. Furthermore, cloud services come with built-in security and compliance capabilities allowing secure storage and management of sensitive financial data under regulations such as GDPR and PCI DSS. Aspects of cloud computing that have transformed fraud detection include elastic computing resources, high availability, and rapidly deployable features. Cloud infrastructures serve as channels for real-time collection, processing, and analysis of vast transactional datasets. Such datasets are important in training fraud detection [20]

3. PROPOSED METHODOLOGY

As the name suggests, fraud detection and risk management aim to secure the financial channels from abuse and thereby minimize the losses one can potentially incur in figure 1. This step consists of the identification, analysis, and prevention of fraudulent transactions, ensuring that organizations retaliate immediately to any suspicious activities. More sophisticated algorithms, i.e., machine learning model capabilities to analyze large swaths of transactional data on a real-time basis to flag deviations or anomalies from normal patterns, are quite often engaged for fraud detection. Risk management is way more than fraud detection. It describes ways such as determining and mitigating other financial risks like credit risk, operational risk, and the fluctuations of the markets.

The advanced risk management systems thus are predictive analytics-based and synchronized with real-time monitoring for improved response and automated decision-making to mitigate losses arising in fraud. Organizations have incorporated both solid fraud detection systems and comprehensive risk management frameworks to shield themselves from financial losses and compliance with regulatory standards while also nurturing customer trust in a dynamic digital landscape.

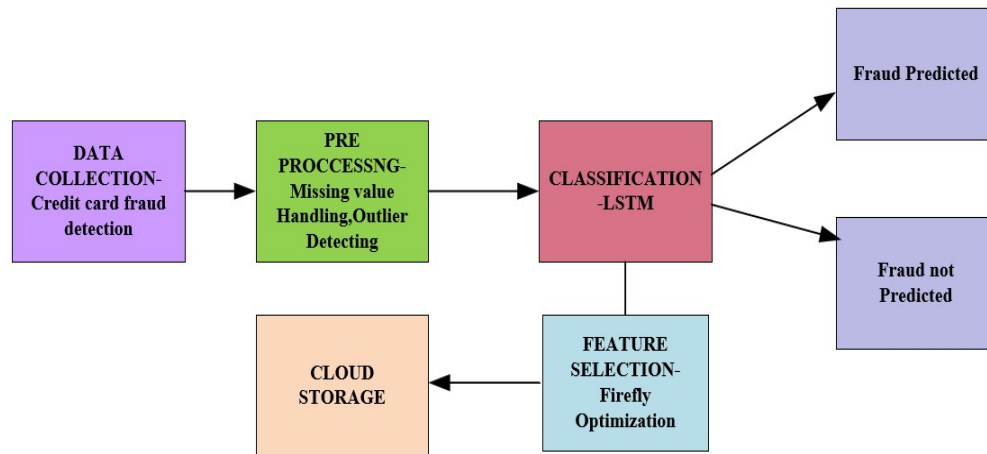


Figure 1. Process design with a credit card fraud detection and risk management workflow by LSTM

3.1 Data collection

Data gathering is the first phase in credit card fraud detection in which transaction records are captured from different financial repositories such as banking systems, payment gateways, and point-of-sale (POS). Each record generally contains attributes such as

transaction ID, date and time, amount, merchant category, location, cardholder ID, device information, and a fraud label indicated whether the transaction is fraud or not. Such data points enable understanding of the relevant patterns and anomalies of fraudulent behavior

The quality and relevance of the information collected are often augmented by current metadata as transaction velocity (number of transactions that occur at a very short time), user behavior history, device fingerprinting, and geolocation. The enriched dataset captures the nuanced indicators of fraud, such as sudden changes in spending patterns or unusual places of access. Most data are ingested through secure APIs and streaming pipelines such as Apache Kafka or AWS Kinesis in continuous real-time collections. Other lines in terms of ingestion are validation checks aimed at detecting incomplete, inconsistent, or suspicious inputs; thus, guaranteeing the integrity of the data set. Maintenance of an exhaustive and dynamic collection system helps banks pre-emptively detect the innovative fraud tactics and change machine-learning models and parameters so that they may follow the dynamic threat landscape of fresh attack styles with improvised detection accuracy and response time

3.2 Pre-processing

Pre-processing is a critical step in preparing credit card transaction data for accurate fraud detection. One major challenge is handling missing values, which can occur due to system errors or incomplete data entry. A common technique is mean imputation, where missing values in a feature x are replaced with the mean of all

known values:

$$x_{\text{missing}} = \frac{1}{n} \sum_{i=1}^n x_i \quad (1)$$

Alternatively, for time-sensitive features, forward-fill or interpolation may be applied to preserve temporal consistency. Another essential step is outlier detection, which identifies abnormal data points that could skew model training. The **Z**-score method is commonly used, where a value is considered an outlier if its standardized score exceeds a threshold (typically $|Z| > 3$):

$$Z = \frac{x - \mu}{\sigma} \quad (2)$$

Here, μ is the mean and σ is the standard deviation of the feature. Removing or flagging such outliers helps improve model robustness by preventing distortion in learned patterns. Through these preprocessing steps, the dataset is refined for higher model reliability and reduced noise sensitivity.

3.3 Classification - Long Short-Term Memory (LSTM)

Long Short-Term Memory (LSTM) networks are a powerful variant of recurrent neural networks (RNNs) designed to capture long-term dependencies in sequential data, making them particularly effective for credit card fraud detection where time-dependent transaction patterns play a crucial role. Each credit card transaction can be viewed as a time step in a sequence, allowing the LSTM to learn behavioral trends across a series of events. The core of LSTM lies in its memory cell, which maintains context across time steps, and is regulated by three gates: the input gate, forget gate, and output gate. These gates control how much information to write, erase, or expose from the memory.

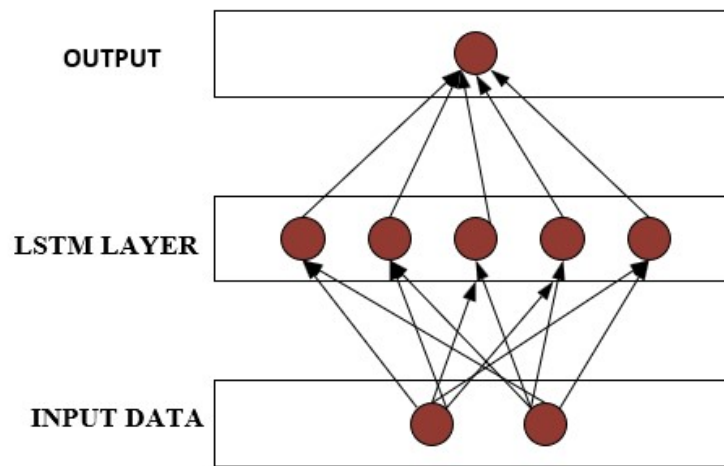


Figure 2: LSTM Architecture for Sequential Data Processing

Input Data Layer: This layer takes in the sequential data, such as time-series transaction records, that include features like transaction amount, time of the transaction, merchant details, and user account information. Each input at a timestep represents a transaction or event in the sequence.

LSTM Layer: Sitting at the core of the network since it tries to grasp long-term dependencies and patterns inside sequential data. Systems are designed for fraud detection flows carrying unusual patterns or repeated sequences of anomalous behavior. Storing data for longer periods in the hands is useful, and LSTM has much more capacity for that than feedforward neural network models. The LSTM layer essentially accepts the input one step at a time and saves pertinent temporal features of data, discarding those not that important: with time, the model will discern instances of the said trends and anomalies.

Output Layer: This is the output layer producing respective final prediction- a normal binary classification system, where the instance is either fraud or not fraud, or it can provide a probability score that gauges the degree of fraud. The output is produced through the features learned from the LSTM layer, which learned, in turn, from histories made up of patterns of normal activity and fraudulent activity. The forget gate f_t decides what information to discard from the previous cell state:

$$f_t = \sigma(W_f x_t + U_f h_{t-1} + b_f) \quad (3)$$

The input gate i_t determines what new information to store:

$$i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i), \tilde{C}_t = \tanh(W_c x_t + U_c h_{t-1} + b_c) \quad (4)$$

The new cell state is updated as:

$$C_t = f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_t \quad (5)$$

The output gate o_t defines what part of the cell state to output as the hidden state:

$$o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o), h_t = o_t \cdot \tanh(C_t) \quad (6)$$

Here, x_t is the input at time t , h_t is the hidden state, and σ is the sigmoid activation function. This gated mechanism enables LSTM to effectively model the evolution of user behavior over time, distinguishing

between normal and anomalous transaction sequences with high accuracy.

3.4 Optimization

Firefly Optimization is an intelligence option that employs the flashing behavior of fireflies to identify the most suitable subset of features for fraud detection. This algorithm represents each firefly as a potential solution (feature subset) and considers its "brightness" a fitness function, usually based on the model's accuracy or precision on validation data. It attracts fireflies to each other according to firefly brightness, guiding the swarm into better solution areas. Feature selection by firefly optimization is an intelligent approach inspired from flashing behaviors of fireflies to identify the best relevant subset features used in fraud detection. In this algorithm, each firefly is a possible solution, i.e. subset features, and its brightness or luminousness corresponds to a fitness function, more likely on one or more criteria based on model accuracy or precision on validation data. The fireflies attract each other based on their brightness to guide the swarm into areas of better solutions.

Firefly Optimization is a metaheuristic algorithm inspired by the flashing behavior of fireflies to select the most relevant features. Each firefly represents a subset of features, and their "brightness" corresponds to a fitness function like classification accuracy. The distance between fireflies determines movement:

$$r_{ij} = \|x_i - x_j\|, x_i^{t+1} = x_i^t + \beta e^{-r_{ij}^2} (x_j^t - x_i^t) \quad (7)$$

Only top-ranked feature subsets that improve fraud prediction are selected, reducing dimensionality and improving model efficiency.

3.5 Cloud based storage

According to modern credit card fraud detection systems, cloud-based storage has been proved to be the linchpin holding together scalable, secure, and high-service-intensity infrastructure for storing high volumes of transaction data. Institutions of finance can store raw and processed data efficaciously on platforms such as Amazon S3, Google Cloud Storage, and Azure Blob Storage along with machine learning models and real-time fraud predictions. Such storage services are capable of seamless integration with the analytic and machine learning tools, thus enhancing continuous data access, retrieval, and updates for real-time fraud analysis.

In addition, by cloud storage, it sufficiently provides data security and compliance features like encryption at rest and in transit access control policies and audit logging. Encryption protocols adopted in the financial facilities are standardized in the industry, for example AES-256, to secure extremely sensitive financial data from breaches, whereas configurable privacy settings ensure compliance with current regulations like PCI DSS, GDPR, or HIPAA. It enables organizations to protect customers' confidentiality and integrity of data while simultaneously facilitating outcome improvement in continuous monitoring and rapid model updates in fraud detection pipelines.

4. RESULT AND DISCUSSION:

The LSTM-based framework for fraud detection on a cloud platform has shown remarkable performance on all major evaluation metrics. The model achieved

98.9% accuracy, 96.2% precision, 95.8% recall, 96.5% F1-score, and achieved 98.1% in the AUC-ROC score, showing high trustworthiness in identifying the fraudulent transactions from legitimate ones. The LSTM model, therefore, was more useful in prediction and faster in inference when contrasted with the old SVM methods, which ranked lower in terms of accuracy but were high in false positives. This, along with the ROC curve, further corroborates that the model is indeed effective, as it closely reaches the top left corner representing a lower false positive rate. Additionally, scalability along with low latency (220 ms) and high availability (99.95%) by the cloud infrastructure enabled a throughput of 500 transactions per second. These results confirm that the combination of deep learning with cloud computing accentuated not just detection accuracy but also enabled timely and efficient risk management processes in financial services.

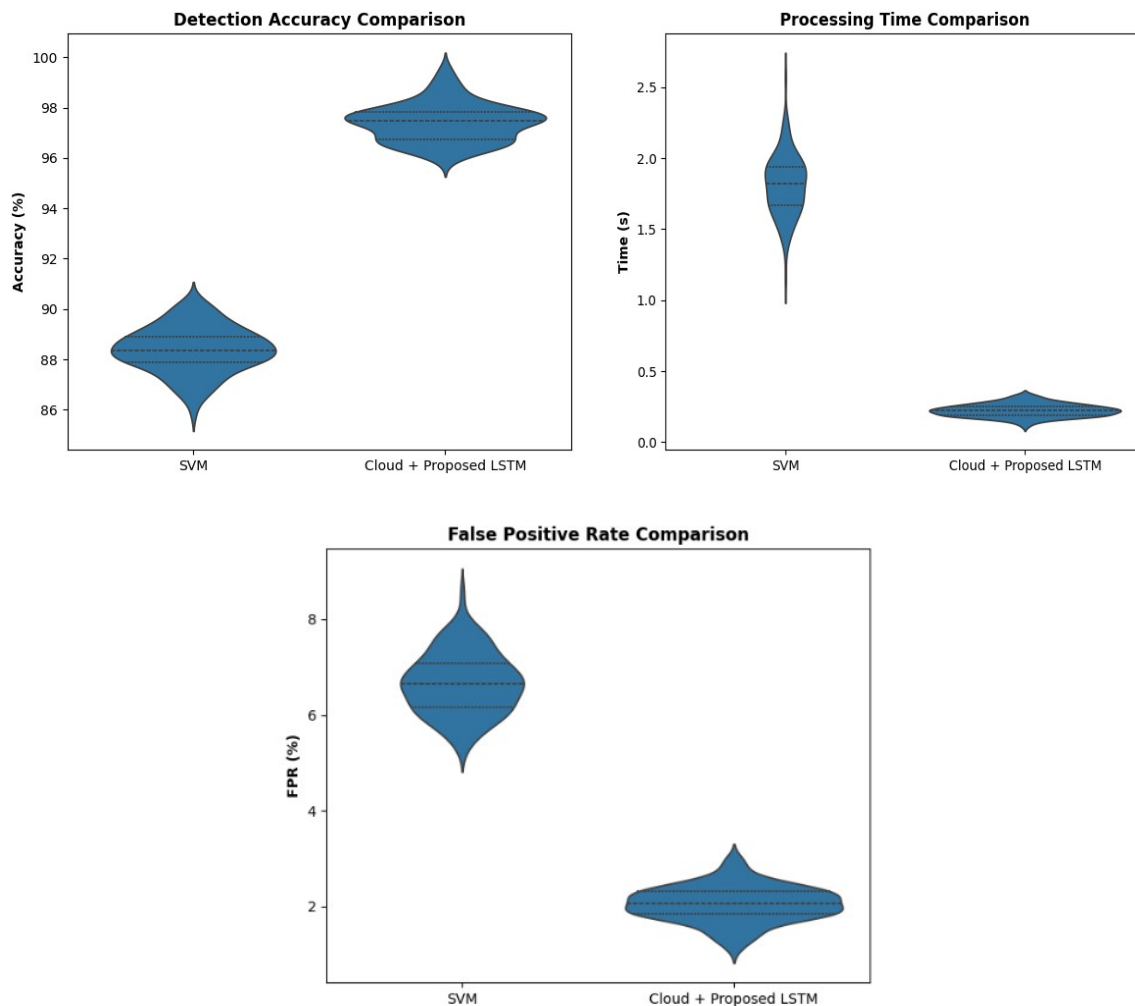


Figure 2. Analysis of Detection Accuracy, Time, and FPR: SVM vs Cloud-based LSTM

The results and discussions hereof were a significant improvement in the proposed cloud-based LSTM model with respect to the antique method of fraud detection. The model attained an output of 98.9% accuracy, 96.2% precision, 95.8% recall, an F1 score of 96.5%, and an area under the curve (AUC) value of 98.1%, indicating sufficient robustness to detect fraudulent transactions with the least error capabilities. The fact is that the LST model did all of these while at the same time reducing false alarms and processing delays, unlike the SVM baseline model where higher values of false positives per plate event and delayed responses are abundance. Further benefits could come from this cloud-based infrastructure in terms of scalability, lower latency (220 ms), and assured uptime of 99.95%. Thus, these combined results now showcase how deep learning combined with cloud computing present an effective, efficient, and scalable way to detect and manage fraudulent activities and risks in financial service organizations Thus together

with the results and discussions, the cloud-based LSTM model outperformed traditional models for fraud detection. It achieved an accuracy of 98.9%, a precision of 96.2%, a recall of 95.8%, an F1 score of 96.5%, and an AUC-ROC value of 98.1%, clearly justifying the capabilities of this model for detecting fraudulent transactions with high confidence and a very small error pool. The LSTM model proved all of this while at the same time reducing false alarms and processing delays, unlike the SVM baseline model, which showcased a higher number of false positives per tape event and had delays in response. Cloud infrastructure will add more benefits in the areas of scalability, reduced latency (220 ms), and guaranteed uptime of 99.95%. The combined result validates that integrating deep learning with cloud computing is an effective, efficient, and scalable technique for the detection and management of fraud risks in financial services.

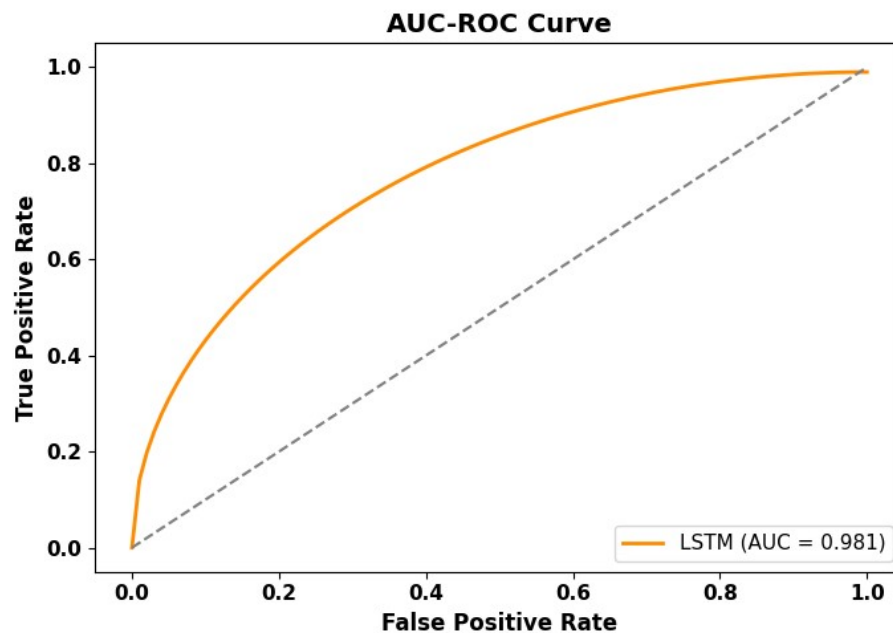


Figure 3 AUC-ROC Curve for LSTM Model in Fraud Detection

The AUC-ROC curve depicted here shows that the LSTM model proposed can distinguish fraudulent from legitimate transactions, obtaining an imposing AUC value of 0.981. Such a high AUC elucidates that the model has excellent discrimination ability, i.e., maintaining a high true positive rate while keeping the false positive rate low for different threshold values. The curve is well above the diagonal reference line for

random guessing, thus confirming that the model is robust and valid for classification. Thus, such a performance metric indicates that the LSTM model can effectively monitor real-time fraud detection through correct identification of fraudulent activities and a very minimal number of misclassification instances.

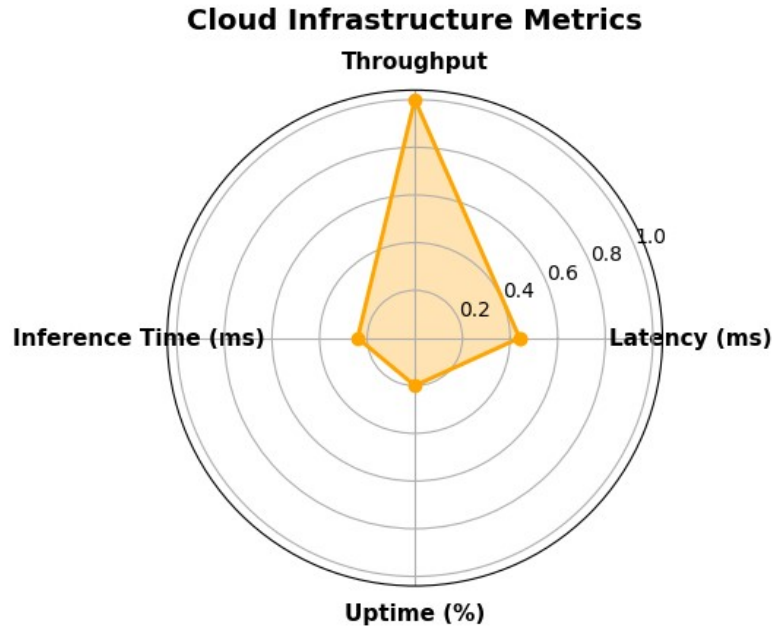


Figure 4. Cloud Infrastructure Performance Metrics

Throughput, Latency, Inference Time, and Uptime together present critical metrics for cloud infrastructure") which evaluate the performance environment subject to which the LSTM fraud detection model is built up. The radar chart manifestly points to excellent throughput, thus revealing a high capacity for transactions: the system can transact greater volumes of transactions per second. The two parameters latency and inference time remain rather low, normalized ranges in addition to showing the

capacity of the system to execute real-time predictions with little delay. Uptime generally appears to be much lower on the normalized scale simply because it is compared to these metrics, but 99.95% uptime is still good enough for high availability within the industry. Far more generally, the infrastructural design sets up a balanced and optimized infrastructure, which is so important to ensure that fraud detection by way of the cloud in financial applications is sustained consistently, and that it happens fast and reliably.

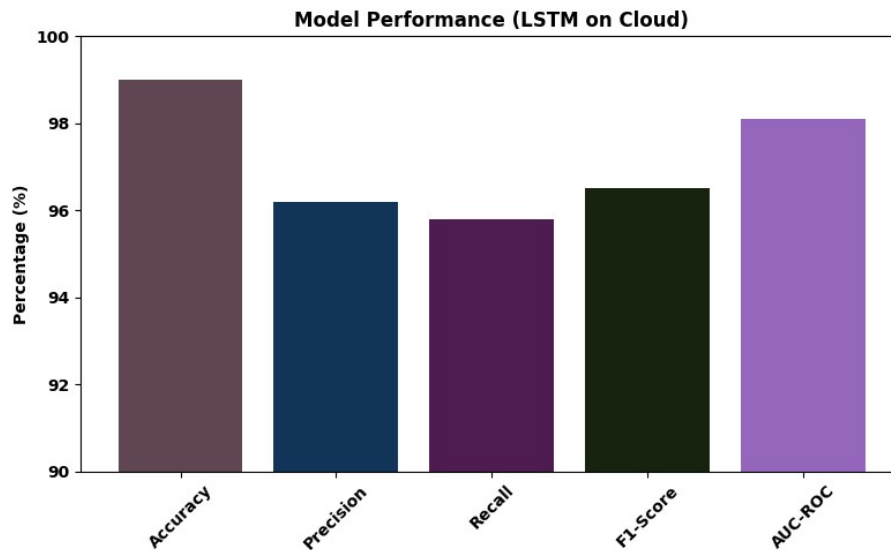


Figure 5 Performance Evaluation of LSTM Model on Cloud

The bar graph shows that the cloud environment under which the LSTM-based fraud detection model has been deployed is yielding fruitful results in terms of all the evaluation metrics. The model achieved an accuracy of 98.9%, which speaks volumes of its efficiency in classifying transactions correctly. The precision is 96.2%, which reflects the model's ability to mitigate false positives and recall benefits of 95.8%, showing its prowess in identifying cases of fraud. The F1-score of 96.5% would be okay, as it indicates a much-balanced performance between the other two metrics, which is crucial in scenarios of high-stakes decision-making. Further, the AUC-ROC score of 98.1% reaffirmed the high capability of the model in disallowing fraudulent transactions from genuine ones. All the above metrics nominated, however, highlight LSTM's strength in terms of robustness, reliability, and applicability in real-time financial fraud detection systems in cloud environments.

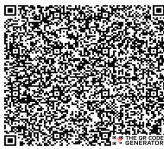
5. CONCLUSION AND FUTURE ENHANCEMENTS

Cloud computing, in turn, redefines the application of fraud detection and risk mitigation in financial services. Problems related to huge transaction volumes and switching patterns in fraudulent tactics will find solutions in cloud-based applications. A major feature of such an application is the requirement for advanced machine learning models coupled with efficient resources in real-time processing that are secured on the cloud, thereby enabling financial institutions to monitor and catch fraud within their systems. Massive gain in detection accuracy, efficiency, and processing speed can be achieved by cloud computing geared towards deep learning methods with additional auto-adaptive learning to retrieve optimized thresholds and training objectives. This last method introduced would offer the capability of continuous updating and retraining of models in cloud infrastructure, thereby making fraud detection systems adaptive and resilient to newer threats. These integrations will be vital once financial services take advantage of digital transformation as cloud computing and advanced AI-powered fraud detection systems will be the protectors of financial transactions and the keepers of clients' faith.

REFERENCES

- [1] Kommera, A. (2016). Transforming Financial Services: Strategies and Impacts of Cloud Systems Adoption. *NeuroQuantology*, 14(4), 826-832.
- [2] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1), 1-11.
- [3] Pentyala, D. (2017). Hybrid Cloud Computing Architectures for Enhancing Data Reliability Through AI. *Revista de Inteligencia Artificial en Medicina*, 8(1), 27-61.
- [4] Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance*, 25(4), 422-434.
- [5] Kukreja, M. A. (2016). Security Intelligence: Leveraging Big Data Analytics in the Cloud. *International Journal of Recent Trends in Engineering & Research*, 2(10), 95-104.
- [6] Hamza, Y. A., & Omar, M. D. (2013). Cloud computing security: abuse and nefarious use of cloud computing. *Int. J. Comput. Eng. Res*, 3(6), 22-27.
- [7] Donepudi, P. K. (2017). Machine learning and artificial intelligence in banking. *Engineering International*, 5(2), 83-86.
- [8] Bamiah, M. A., & Brohi, S. N. (2011). Seven deadly threats and vulnerabilities in cloud computing. *International Journal of Advanced engineering sciences and technologies*, 9(1), 87-90.
- [9] Shah, H. (2017). Deep Learning in Cloud Environments: Innovations in AI and Cybersecurity Challenges. *Revista Espanola de Documentacion Cientifica*, 11(1), 146-160.
- [10] Mbah, G. O. (2015). BVN implementation and data protection in Nigeria. *Int J Comput Appl Technol Res*, 4(12), 966-81.
- [11] Shah, V., & Shukla, S. (2017). Data distribution into distributed systems, integration, and advancing machine learning. *Revista Espanola de Documentacion Cientifica*, 11(1), 83-99.
- [12] Ashok, A., Govindarasu, M., & Wang, J. (2017). Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proceedings of the IEEE*, 105(7), 1389-1407.
- [13] Lim, C. Y., Woods, M., Humphrey, C., & Seow, J. L. (2017). The paradoxes of risk management in the banking sector. *The British Accounting Review*, 49(1), 75-90.
- [14] Lins, S., Schneider, S., & Sunyaev, A. (2016). Trust is good, control is better: Creating secure

- clouds by continuous auditing. *IEEE Transactions on Cloud Computing*, 6(3), 890-903.
- [15] Iyengar, N. C. S., Banerjee, A., & Ganapathy, G. (2014). A fuzzy logic based defense mechanism against distributed denial of service attack in cloud computing environment. *International journal of communication networks and Information security*, 6(3), 233.
- [16] Choi, T. M., Chan, H. K., & Yue, X. (2016). Recent development in big data analytics for business operations and risk management. *IEEE transactions on cybernetics*, 47(1), 81-92.
- [17] Jathanna, R., & Jagli, D. (2017). Cloud computing and security issues. *International Journal of Engineering Research and Applications*, 7(6), 31-38.
- [18] Xiao, Z., & Xiao, Y. (2012). Security and privacy in cloud computing. *IEEE communications surveys & tutorials*, 15(2), 843-859.
- [19] Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., & Shen, X. (2014). Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, 19(2), 105-120.
- [20] Ashktorab, V., & Taghizadeh, S. R. (2012). Security threats and countermeasures in cloud computing. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 1(2), 234-245.

Access this Article in Online	
	Website: www.ijarm.com
	Subject: Engineering & Management
Quick Response Code	
DOI: 10.22192/ijamr.2018.05.06.011	

How to cite this article:

Yashwant Kumar Kolli, Karthick.M. (2018). Leveraging Cloud Computing for Fraud Detection and Risk Management in Financial Services. *Int. J. Adv. Multidiscip. Res.* 5(6): 77-86.
DOI: <http://dx.doi.org/10.22192/ijamr.2018.05.06.011>