Journal of Artificial Intelligence, Virtual Reality, and Human-Centered Computing
ISSN: 3069-2318

PRIME OPEN ACCESS

Volume 2, Issue 2

Research Article

Date of Submission: 03 Mar, 2026
Date of Acceptance: 31 Mar, 2026
Date of Publication: 08 Apr, 2026

Advancing Insider Threat Detection: A Novel Framework for Enhanced Security in Cloud Computing Environments

Segun Kazeem Fatoki[1], Olalekan Akinbosoye Okewale[1*], Mayowa Oyedepo Oyediran[1], Olufemi S Ojo[1] and Olugbenga Ayomide Madamidola[2]

[1]Department of Computer Science, Ajayi Crowther University, Nigeria

[2]Department of Information Technology School of Computing, The Federal University of Technology Akure Ondo State, Nigeria

***Corresponding Author:** Olalekan Akinbosoye Okewale, Department of Computer Science, Ajayi Crowther University, Nigeria.

Citation: Fatoki, S. K., Okewale, O. A., Oyediran, M. O., Ojo, O. S., Madamidola, O. A. (2026). Advancing Insider Threat Detection: A Novel Framework for Enhanced Security in Cloud Computing Environments. *J AI VR Hum Comput, 2*(2), 01-08.

Abstract

Insider threats are major security issues in cloud computing where legitimate users with privileged access misuse their credentials to attack data, systems, or services. Conventional intrusion detection systems are ineffective for insider threat detection in cloud computing since they are based on predefined rules or signatures that are not well-suited for cloud dynamics. In this study, a novel insider threat detection model for cloud computing is proposed by combining the capabilities of convolutional neural networks (CNN) and gated recurrent units (GRU) to extract both spatial and temporal information from the Community Emergency Response Team (CERT) insider threat dataset containing 30,000 samples from Carnegie Mellon University. The proposed CNN-GRU hybrid network performs better with an accuracy of 99.8%, a sensitivity of 99.7%, and a lowest false negative rate of 0.002%, outperforming the accuracy of 96.98% achieved by CNN and the accuracy of 95.91% achieved by LSTM.

Keywords: Cloud Computing, Insider Threat Detection, Convolutional Neural Networks (CNN), Gated Recurrent Unit (GRU), Deep Learning, Information Security Management

Introduction

Cloud computing is essentially the remote delivery of data and application services over the internet, in contrast to storing data in local hard drives or in-house infrastructure. With internetbased connectivity, cloud computing allows users to tap into a variety of computing resources such as servers, networks, storage, applications, and services Raut et al., 2020 [1]. These are shared between different users in a manner that is dynamically allocated and released based on demand. With cloud computing, users are provided with the benefit of accessing their files and applications from any device with internet connectivity. Google's Gmail is a cloud computing service bhushan01. The National Institute of Standards and Technology (NIST) considers cloud computing to be a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, apps, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction goggi2019semantic.

The widespread use of cloud computing has fundamentally changed the IT landscape in many ways: it offers scalability, cost-efficiency, the ability to manage resources centrally, location independence, and risk mitigation. The use of cloud infrastructures and shared environments brings a number of security challenges, such as privacy, data location, malicious insiders, and vendor lock-in Mandal and Chatterjee, 2015 [2]. Insider threats are a significant challenge to the adoption of cloud computing, and they refer to a situation in which an authorized user takes advantage of their privileged access

to compromise system integrity, steal sensitive data, or cause disruption of cloud services Mandal and Chatterjee (2015) [2]. Cloud computing fundamentally changes the traditional understanding of data storage and processing by distributing resources and using remote servers accessed over the Internet, creating a complex set of security vulnerabilities and having data cross networks Yanamala, 2024 [3].

With organizations racing to protect sensitive data and critical assets against malicious insiders, insider threat detection is viewed as an issue of paramount importance Alzaabi and Mehmood, 2024 [4]. Prior works have focused on machine learning and deep learning techniques for the detection of insider threats in clouds. It is expected that the self-learning capabilities of deep learning networks may enhance detection further and help in improving class imbalance issues shanmugapriya2024cloud. According to a 2022 Cloud Security Report, insider attacks account for about 35% of cloud data breaches across the world. Therefore, insider threat detection in clouds is very important for ensuring data confidentiality, integrity, and business continuity Reddy et al., 2025 [5].

Detecting internal threats is difficult because these insiders already have valid access to sensitive information and system vulnerabilities. Classic IT security depends mostly on external threats with rule-based, signature-based intrusion detection and fails to consider the potential threat insiders can cause by exhibiting abnormal behavior while possessing legitimate privileges A. Duncan et al., 2015 [6].

For cloud security, the same negligence towards insider threat detection has been observed using signature-based detection systems. These methods tend to often miss the insider threats that rightfully possess access and can exhibit anomalous behavior Jang-Jaccard and Nepal, 2014 [7]. This identifies the gap mentioned and states that detection mechanisms should be exclusively designed against insider threats since classic methods aren't well-positioned to meet such subtle challenges Alsowail and Al-Shehari, 2020 [8].

Cloud-based security has been found challenged by the problem of insider threats. These individuals are well versed with the inner workings of the system and, therefore, can evade the normal safety measures set up for threat protection and cause harm. Thus, failing to address the problem by the design of models for insider threat detection exposes the system to breaches, loss of IP, and interruption of services with associated high financial losses and reputational damage Mandal and Chatterjee, 2015 [2]. Insider threat detection is a challenge because the attackers are legitimate and therefore already have access, are well versed with the vulnerability of the system, and are able to conceal their acts of maliciousness. The gap among the challenges of cloud-based security will be addressed by the design of a hybrid insider threat detection model for the cloud system that combines convolutional neural networks and GRUs for analysis Nicolaou et al., 2020 [9].

The need for a stronger insider threat detection method for cloud computing was made possible by proposing a novel method that utilizes Convolutional Neural Network (CNN) and Gated Recurrent Units (GRU). Several insider threat designs have been developed and utilized for protection against multiple threats in a cloud setup. The designs regularly use CNNs for threat modeling Nicolaou et al., 2020; however, CNN designs may have limitations in accuracy and a greater number of false negatives owing to their parameters George and Sagayarajan, 2023 [9,10]. Despite advancements in the threat detection domain, there remains a critical vacuum in addressing insider threats to the cloud computing environment using a combination of more than one deep learning algorithm to form a hybrid approach Al-Mhiqani et al., 2020 [11]. Existing research predominantly concentrates on external threats, disregarding the potential for malicious activities initiated by individuals with authorized access privileges Cao et al., 2022; this oversight leaves cloud systems susceptible to secret and complicated insider threats [12].

Related Works

George and Sagayarajan (2023) show the risk of insiders acting maliciously in both government and private sectors and present a new way to find such actions [10]. They use text samples from users' log data at a detailed level, which they turn into character embeddings and a deep learning model with a CNN and LSTM. They test their approach on part of the CERT Insider Threat dataset, r4.2, and get high precision and recall. But they need more tests on different datasets and real situations to check the model's strength.

The adoption of cloud services has a significant impact on the security stance of organizations and critical infrastructure; thus, it is crucial that new threats and risks generated by this new model are comprehensively understood and counteracted Kandias et al., 2011 [13]. The cybersecurity industry is well-versed in the concept of a malicious insider. A malicious insider in the cloud could potentially have access to an unprecedented volume of information on a significantly larger scale because of an authorized access to the data and cloud environment A. J. Duncan et al., 2012 [14].

George and Sagayarajan (2023) tackle the problem of insider threats and the limitations of conventional security measures for safeguarding organizational assets [10]. This study examines various ways to build a model that can reduce vulnerability to insider threats and suggests a machine learning model based on bio-inspired computing using an unsupervised learning algorithm for anomaly detection. This study shows the benefits of swarm intelligence algorithms for enhancing model performance. The results show that swarm intelligence algorithms are good at feature selection optimization producing near-optimal subsets of features. However, future work should test the model's practicality and

possible drawbacks.

An unsupervised user behavior modelling technique using an LSTM-based autocoder to identify insider threats was proposed by aktar2022network<empty citation>. However, the approach has some limitations, such as the dependence on a threshold based on the reconstruction error of a normal dataset, which may be affected by data variations. Testing of the CERT insider threat showed promising outcomes but a noticeable false positive rate. Future work can aim to improve the model's ability to handle new behavior patterns and fine-tune the thresholdsetting process to reduce false positives, thus enhancing the overall reliability of the proposed technique.

The authors Ahsan and Nygard (2020) dealt with security issues in cloud computing that arose from the growing use of cloud services for data storage [15]. They suggested an intrusion detection system (IDS) that uses network traffic monitoring to keep system performance. This paper presents a hybrid method that combines Cuckoo Search (CS) as an optimization algorithm with feedforward back propagation neural network (FFBPNN) as a multi-class classification technique. The CS is applied to select important features from user access requests to cloud data, which reduces training time and complexity. The experimental analysis showed moderately high precision (85.5%), recall (86.4%), F-measure (85.9%), and accuracy (86.22%) for the proposed system, exceeding the existing methods.

Oladimeji et al. (2021) tackle the problem of identifying malicious actions from insiders who can bypass usual security measures [16]. They use behavioral analysis to separate normal and malicious activities and apply a deep learning method to insider threat detection with a rich feature set. They test on the CMU CERT synthetic insider threat dataset r4.2 and get good results, with their algorithm achieving 90.60% accuracy, 97% precision, and 94% F1 score. However, they do not examine possible limitations of their algorithm. Future work could improve by testing its robustness on different datasets and verifying its usefulness in real-world settings through practical applications.

Liu and Lang (2019) investigated the problem of uneven data distribution in identifying malicious insiders with machine learning methods [17]. Uneven data distribution happens when there is a large discrepancy in the amount of data between malicious and legitimate users, resulting in errors by ML models. Previous research on MIT identification has not examined various sampling techniques, such as reducing or increasing the sample size. The proposed double-layer structure, using NM-2 and one-class SVM, achieved recall and f-scores of 100% and 78.72%, respectively, showing outstanding detection of MIT. It also shows an accuracy of 82.46%, which indicates a reasonable overall detection rate for malicious insider threats.

Rana et al., 2022 examined four intrusion detection systems on attack patterns through the use of NSL-KDD and UNSW-NB15 datasets [18]. The study brings forth the ever-increasing complexity of protecting user data and provides recommendations to fill this security gap. The results indicate the effectiveness of a hybrid model incorporating an SVM classifier over other approaches for the datasets upon which this study focused. Insider threats are ever-increasing for corporate security, and a conceptual model for addressing this problem was presented by Tsimenidis et al., 2022 [19]. The model described can be broken down into a number of points including the collection of log files. Then, processing logs to enable the creation of user-centric sequences of events per day. Further recommendations provided by this study make use of a GRU model for detecting insider threats. The results stage shows the classification model's outcomes, which help to find malicious behavior in an organization. Although the suggested way is promising, future work will test its effectiveness on real and public datasets. Also, the use of a modified adaptive synthetic oversampling technique called the adaptive synthetic oversampling technique (ADASYN) algorithm is recommended to handle imbalances in insider threats. These enhancements further increase the way's suitability and reliability in realistic security scenarios.

George and Sagayarajan (2023) presented a novel two-layer approach to MIT detection by integrating ML based on SVM classifiers with anomaly-based MIT detection (AMITD) models [10]. However, they emphasized the importance of ensuring synchronization between the training data and the testing data while introducing a novel approach called NM-2, which performed much better in terms of precision, recall, F-score, and overall accuracy than other sampling methods. For stage one, George and Sagayarajan designed a system for processing, converting, and sampling from the CERT v3.2 dataset by using various undersampling and oversampling strategies, and concluded that NM-2 performed best [10]. The balanced dataset is utilized for the training of a one-class SVM classifier. For evaluating the AMIDT system, they utilized a confusion matrix and parameters like accuracy, precision, recall, and F-score. Accordingly, it is seen that the proposed OC-SVM–based approach outperforms the previous methods with a recall of 100%, an F-score of 78.72%, and an accuracy of 82.46%. Compared with previous state-of-the-art approaches that include deep learning algorithms and boosting algorithms, the proposed system may have a lower total accuracy measure than some other competitive approaches; however, it may have a higher recall value and F-score that represents efficient MIT detection performance. Researchers have argued that a double-layer system diminishes previous limitations associated with MIT detection performance and stressed that it is significant to emphasize that their OC-SVM-based anomaly detection system is significant. For improvement of efficiency and successful mitigation of previous limitations, it is recommended by these researchers that a hybrid system may be considered in comprehensive system design.

Research by Villarreal-Vasquez et al. (2021) highlights the presence of insider threats—misuse of privileges and knowledge in furthering various attacks [20]. The authors note the difficulty in identifying the insider threats using

today's security measures because the insiders mix the attack activities with the legitimate ones in a way that obscures the sequences in the logs security systems check for detection. To address the threat, the authors propose the use of LADOHD—an LSTM-based anomaly detection method designed to learn sequences associated with legitimate activities in a computer system while allowing it to identify attack activities happening over a longer period of time. LADOHD was tested using 38.9M events from a 30-machine commercial network over 20 days while using the network for four days in insider threat attacks. The success of the project was determined using accuracy at 95.91%, precision at 99.50%, recall at 96.12%, and a 0.38% rate of FP—all of which were higher than the existing standards using the method of anomaly detection.

Shivhare et al. (2023) describe in detail the step-by-step process of insider threat detection in an organizational security, which has emerged as a major concern these days. Diverse sources of data were acquired [21]. They structure this log data into a series of sequences for each distinct person on a daily basis. They use a gated recurrent unit approach for insider threat identification. In their result analysis step, their Insider Threat Identification Technique uses classification results to indicate malicious activities inside any organization. The technique looks promising but will be validated for realistic examples from public datasets. They also propose to modify their ADSYN algorithm to handle insider threat classification with imbalanced classes.

Padiet et al. (2023) are specifically discussing insider threat detection by looking at user activity [22]. The authors introduce a deep learning algorithm with a high accuracy rate while maintaining a low false positive ratio. The research uses a malicious insider attacks synthetic data set from CMU CERT r4.2. The experimentally evaluated algorithm called LMT demonstrates high accuracy (99.6%) in comparison with previous models.

sivakrishna2023aubit<empty citation> proposes a pattern-driven insider threat classification approach using a co-evolutionary neural network (CNN). Being designed as a predictive model, the approach utilizes features that lack spatial correlation. Combining spectral and spatial analyses allows the differentiation of insider threats from image-based representations of user activity logs. The proposed method reduces all the scenario-specific single-day features into a single 1D feature vector and then converts this single 1D feature vector into images, where the visual pattern can be leveraged by WCNN to detect malicious insiders. Then, for handling class imbalance issues, this method utilizes the SMOTEENN sampling technique. The authors applied their approach to a benchmark dataset, and the results prove to have outperformed the current state-of-the-art techniques with 97.19% classification accuracy and a recall of 97.30%, offering a very low insider threat detection rate of false positives.

The various studies that were reviewed showed that the insider threat detection models did not have enough accuracy for real-time threat identification in a cloud system. Therefore, it is essential to address the common problem with high recognition accuracy. The research presented a solution that could deal with the problems stated in the existing study. The hybrid CNN– GRU model combines the advantages of both CNN and GRU architectures. While the CNN model is good at spatial pattern recognition, it has limitations due to its sensitivity to hyperparameters (e.g., filter count, size, stride, padding, and pooling). On the other hand, the GRU model, which is good at handling sequential data, may miss some spatial patterns that are relevant to insider threat detection automatically mark attendance, which saves time and reliability.

Methodology

The methodology employs the combination of two deep learning techniques - convolutional neural networks (CNN) and gated recurrent units (GRU) model as the core system used to detect insider threat from community emergency response teams. These two models are leveraged for its effectiveness in cloud computing to address the gaps presented from previous research work that uses only CNN or LSTM model.

Data Collection and Description

This research used the CERT Insider Threat Dataset, which has been offered by the Computer Emergency Response Team. The dataset has been sourced from Carnegie Mellon University, covering approximately 82.7 GB data. The dataset includes records of computer activity of employees in an organization, including logins, system activity, HTTP/file, and emails, along with information relevant to an organization, including departments.

Preprocessing and Feature Extraction

Preprocessing mainly consists of a couple of important steps that keep the consistency of the dataset intact. First, data cleaning: trimming away the irrelevant bits, spotting incomplete or missing values, and removing duplicates. Then, data transformation: turning the raw data into a clean, standardized format that's ready for analysis, reporting, and informed decision-making.

Model Development

The CNN-GRU approach combines the strength of both worlds, leveraging the power of convolutional neural networks to identify spatial relationships and gated recurrent units to track temporal connections. As illustrated in Figure 1, the GRU layer is positioned after the CNN layers in the network. This configuration begins with layers of CNN to extract local features from the user sequence data (the vector matrix), followed by a layer comprising a GRU to process those features over time. A GRU layer can be modeled mathematically by these equations:

$$F = \text{CNN}(X) \tag{1}$$

$$H = \text{GRU}(F) \tag{2}$$

where:
• CNN(X) represents CNN layer
• GRU(X) represents the GRU layer.

The input data, denoted X, represents a time sequence of vectors formulated as a matrix. Using the series of CNN layers, X is transformed into a series of feature maps. We define this series of feature maps as F. The series of feature maps is further processed by a GRU layer. The output of this layer is a series of hidden states denoted H. A fully connected layer takes this series H as input and produces an output. The mathematical formulation of this CNN-GRU neural network model is given by:

$$\text{Output} = \text{FC}(H) \tag{3}$$

where:
• FC(H) represents the fully connected layer

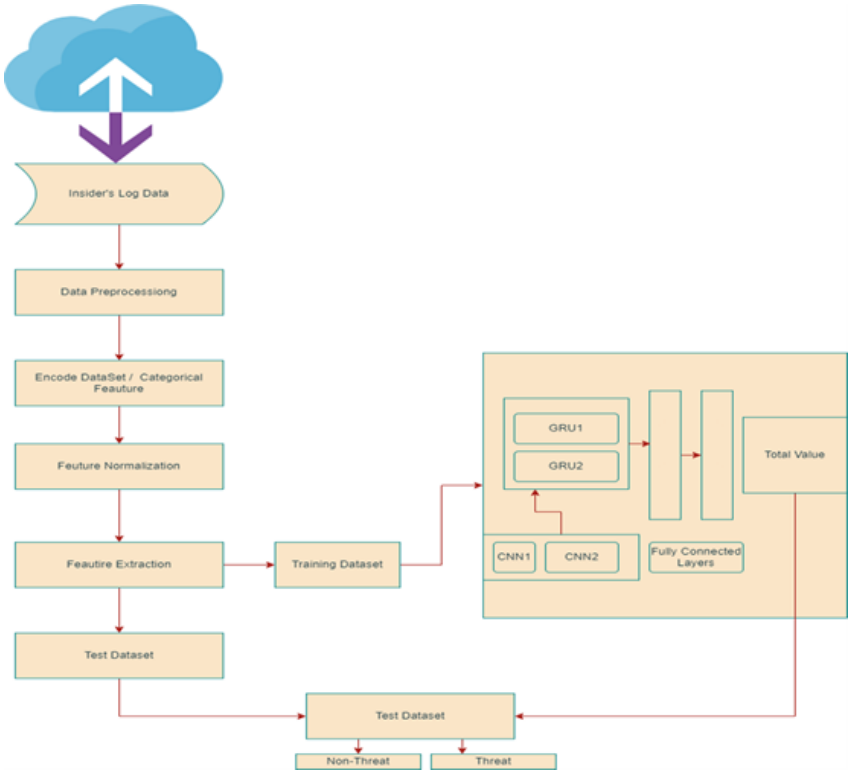


Figure 1: CNN—GRU Architecture

Dataset Split

The data consisting of 30,000 entries is divided into three sections: training, validation, and test data. In the initial division, 80% is allocated for training and validation purposes, with 20% for validation. In turn, for training purposes, 90% is used for training data and 10% for test data.

Evaluation Metrics

Various metrics have been used to check the performance of models:
• **Accuracy:** The correctness of the model.
• **Precision:** The accuracy of the model in identifying the positive sample
• **Recall:** Ability to detect insider threat

Results and Discussion

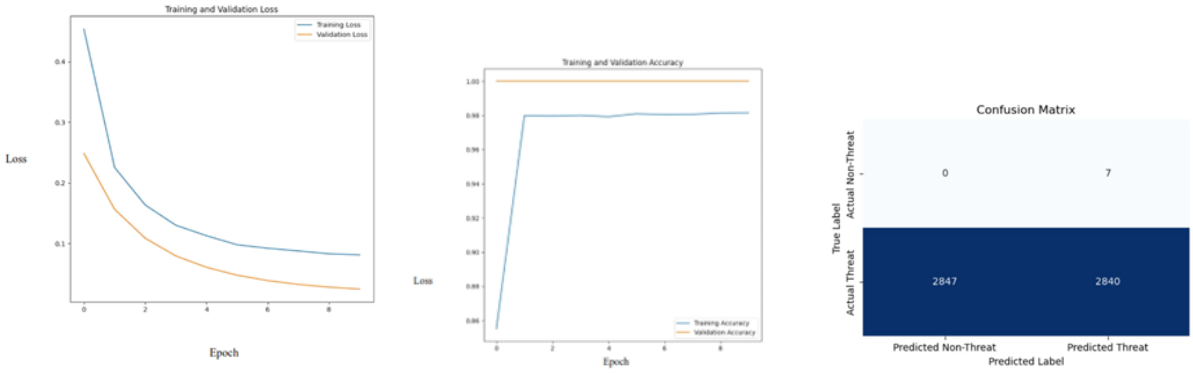
The study's findings are displayed in a number of tables and figures that show how well the created model detects insider threats.

Validation Loss

Figure 2 below shows the validation error for the series of epochs, and it is evident that it reduces continually, from a value of 0.4539 in the initial epoch to a nominal value of 0.0812 in the tenth epoch.

Training Accuracy

The accuracy on the training data rises from 0.8550 to 0.9816 in the tenth epoch, and this highlights how efficiently the model learns about insider threats. The accuracy on the validation data remains perfect at 1.00 all through the training process as shown in Figure 2.



(a) Validation Loss (b) Accuracy (c) Confusion Matrix

Figure 2: Model Performance Metrics

The above confusion matrix from Figure 2 shows that the system is capable of classifying non-threats and threats separately. Notice that CNN-GRU performed outstandingly well with an actual 2,840 threats and 7 non-threats against actual values of 2,847 threats and 0 non-threats.

Test Evaluation

The assessment on the distinct testing dataset gives insights into how well the model performs in reality. Table I highlights the training and testing metrics over ten epochs. The decreasing losses and increasing accuracy of the model indicate that it's progressing in the right direction. Table II highlights the testing accuracy of the model to be 99.8%.

Comparison with Other Models

A comparison of the models designed by Qasim and Alslaiman with that of Callegati, with respect to 2018, as illustrated in Figure 3., reveals the superiority of the CNN-GRU combination over the models based on CNN and LSTM architectures. The combined strategy performs outstandingly in each case, with a test accuracy of 99.8%, precision of 99.7%, recall of 99.7%, and an FNR of 0.002%.

Epoch	Loss	Accuracy	Val_Loss	Val_Accuracy
1	0.4539	0.8550	0.2483	0.8500
2	0.2255	0.9799	0.1564	0.8700
3	0.1635	0.9796	0.1086	0.8800
4	0.1300	0.9800	0.0793	0.8900
5	0.1127	0.9792	0.0606	0.9000
6	0.0978	0.9810	0.0475	0.9100
7	0.0920	0.9805	0.0387	0.9200
8	0.0876	0.9806	0.0324	0.9300
9	0.0829	0.9814	0.0279	0.9400
10	0.0812	0.9816	0.0246	0.9500

Table 1: Training and Evaluation Metrics

Model	Accuracy (%)	Recall (%)	Precision (%)	FNR (%)
CNN–GRU	99.80	99.70	99.70	0.002

Table 2: Test Results

The results decisively establish the efficacy of the strategy and its applicability in different scenarios, thus verifying the strategy as a reliable solution for insider threat detection in cloud computing systems.

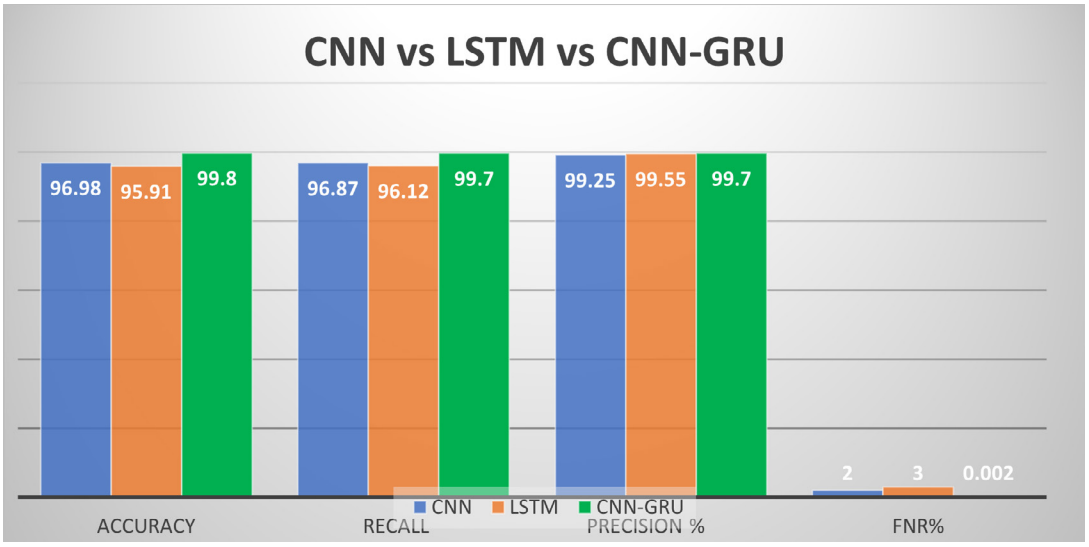


Figure 3: Result Comparison

Conclusion

The combination of a convolutional neural network (CNN) and Gated Recurrent Units (GRU) has assisted in improving insider threat detection in a cloud computing environment. The CNNGRU method utilizes CNN's ability to identify spatial features and GRU's aptness in handling sequential values, thus coping with limitations of previous insider threat detection mechanisms.

Experiments on the CERT dataset provided by Carnegie Mellon University prove its resilience, leading to continuous enhancement on metrics such as accuracy, precision, and recall.

This experiment confirms that the proposed architecture would be significantly affected by its proficiency to identify complex insider threat behaviors in cloud setup scenarios.
It is evident that the integration of spatial, as well as time-based feature learning, is an important step forward in cloud security. Looking into the future, there are expectations that research efforts in the coming days would focus on increasing efficiency, adaptability, and its interaction with security systems.

References

1. Raut, M., Dhavale, S., Singh, A., & Mehra, A. (2020, December). Insider threat detection using deep learning: A review. In 2020 3rd international conference on intelligent sustainable systems (ICISS) (pp. 856-863). IEEE.
2. Mandal, K. K., & Chatterjee, D. (2015). Insider threat mitigation in cloud computing. International Journal of Computer Applications, 120(20).
3. Yanamala, A. K. Y. (2024). Emerging challenges in cloud computing security: A comprehensive review. International Journal of Advanced Engineering Technologies and Innovations, 4(1), 448-479.
4. Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access, 12, 30907-30927.
5. Reddy, A. Y., Yashwika, B., Kumar, B. K., Teja, R. S. D., & Shreyas, K. (2025). REAL-TIME INSIDER THREAT DETECTION IN CLOUD PLATFORMS THROUGH ENSEMBLE LEARNING AND USER BEHAVIOR ANALYTICS. International Journal of Data Science and IoT Management System, 4(3), 149-156.
6. Duncan, A., Creese, S., & Goldsmith, M. (2015). An overview of insider attacks in cloud computing. Concurrency and Computation: Practice and Experience, 27(12), 2964-2981.
7. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of computer and system sciences, 80*(5), 973-993.
8. Alsowail, R. A., & Al-Shehari, T. (2020). Empirical detection techniques of insider threat incidents. *IEEE access, 8,* 78385-78402.
9. Nicolaou, A., Shiaeles, S., & Savage, N. (2020). Mitigating insider threats using bio-inspired models. *Applied Sciences, 10*(15), 5046.
10. George, A. S., & Sagayarajan, S. (2023). Securing cloud application infrastructure: understanding the penetration testing challenges of IaaS, PaaS, and SaaS environments. *Partners Universal International Research Journal, 2*(1), 24-34.
11. Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., ... & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. *Applied Sciences, 10*(15), 5208.
12. Cao, B., Li, C., Song, Y., Qin, Y., & Chen, C. (2022). Network intrusion detection model based on CNN and GRU.

Applied Sciences, 12(9), 4184.
13. Kandias, M., Virvilis, N., & Gritzalis, D. (2011, September). The insider threat in cloud computing. In International Workshop on Critical Information Infrastructures Security (pp. 93-103). Berlin, Heidelberg: Springer Berlin Heidelberg.
14. Duncan, A. J., Creese, S., & Goldsmith, M. (2012, June). Insider attacks in cloud computing. In *2012 IEEE 11th international conference on trust, security and privacy in computing and communications* (pp. 857-862). IEEE.
15. Ahsan, M., & Nygard, K. E. (2020, March). Convolutional Neural Networks with LSTM for Intrusion Detection. In *CATA* (Vol. 69, pp. 69-79).
16. Oladimeji, T. O., Ayo, C. K., & Adewumi, S. E. (2021, April). Insider threat detection using binary classification algorithms. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1107, No. 1, p. 012031). IOP Publishing.
17. Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences, 9*(20), 4396.
18. Rana, P., Batra, I., Malik, A., Imoize, A. L., Kim, Y., Pani, S. K., ... & Rho, S. (2022). Intrusion detection systems in cloud computing paradigm: analysis and overview. *Complexity, 2022*(1), 3999039.
19. Tsimenidis, S., Lagkas, T., & Rantos, K. (2022). Deep learning in IoT intrusion detection. *Journal of network and systems management, 30*(1), 8.
20. Villarreal-Vasquez, M., Modelo-Howard, G., Dube, S., & Bhargava, B. (2021). Hunting for insider threats using LSTM-based anomaly detection. *IEEE Transactions on Dependable and Secure Computing, 20*(1), 451-462.
21. Shivhare, I., Purohit, J., Jogani, V., Attari, S., & Chandane, M. (2023). Intrusion detection: A deep learning approach. *arXiv preprint arXiv:2306.07601.*
22. Padiet, P., Islam, R., & Khan, M. A. (2023, May). Analysis of Malicious Intruder Threats to Data Integrity. In *International Conference on Advances in Computing Research* (pp. 359-368). Cham: Springer Nature Switzerland.