**The Eastasouth Journal of Information System and Computer Science**
Vol. 2, No. 02, December 2024, pp. 284-293
ISSN: 3025-566X, DOI: 10.58812/esiscs.v2i02

# Federated Machine Learning for Privacy-Preserving Cyber Threat Intelligence in Global Cloud-Integrated MIS Platforms

**Md Kazi Tuhin[1], Md Talha Bin Ansar[2], Mohammad Somon Sikder[3], Hemayet Uddin Himel[4], Harleen Kaur[5], Hasan Imam[6], Ahmed Shan-A-Alahi[7*]**
[1,2] Yeshiva University, Manhattan, New York, USA
[3,4] Pacific States University, Los Angeles, California, USA
[5] Westcliff University, Irvine, California, USA
[6] International American University, Los Angeles, California, USA
[7] Washington University of Science and Technology, Virginia, USA

**Article Info**

***Article history:***
Received Dec, 2024
Revised Dec, 2024
Accepted Dec, 2024

***Keywords:***
CIC-IDS-2017 Dataset;
Cloud;
Deep Learning;
Federated Learning;
Machine Learning;
Management Information Systems.

**ABSTRACT**

Cyber Intelligence (CI) is an advanced security system that defends networks against cyberattacks by using ML models. In conventional centralized machine learning tools used to detect cyber threats, critical organizational information must be shared, which imposes severe privacy and security issues. To overcome this issue, this paper suggests a privacy-aware cyber threat detection system based on Federated Learning combined with a Convolutional Neural Network (FL-CNN). The proposed framework is tested on CIC-IDS-2017 dataset, where the methods of preprocessing like: missing value imputation, MinMax normalization, one-hot encoding, and attack label remapping are used. Experiment findings show that the suggested FL-CNN model outperforms the centralized CNN model in most metrics, including accuracy (96.8%), precision (96.2%), recall (96.7%), and F1-score (96.5%). Also, a false positive rate of the model stands at 0.025, which is much lower meaning that the model is better at identifying a cyber threat in a distributed cloud system.



***Corresponding Author:***
Name: Ahmed Shan-A-Alahi
Institution: Washington University of Science and Technology, Virginia, USA
Email: aalahi.student@wust.edu

## 1. INTRODUCTION

Within the present-day digital ecosystem, organizations are also increasingly relying on a Management Information System (MIS) that is cloud-integrated with the support of cloud computing in order to support data-driven decision-making processes within a distributed enterprise ecosystem [1]. Attacks in the modern period, such as DDoS, ransomware, data exfiltration, and Advanced Persistent Threats (APTs), exploit security holes in cloud and distributed networks to compromise the confidentiality and integrity of sensitive company information [2]. The emergence of Cyber Threat Intelligence (CTI) has become one of the critical methods of detecting, assessing, and preventing a possible cyber threat by gathering and examining information of a security nature [3][4]. The absence of supervision by the platform's proprietors regarding the data and activities on the platform raises concerns regarding data privacy and security. The security wall is readily breached by assailants, resulting in the destruction of cloud data. Despite the introduction of a variety of privacy protection methods, including encryption, access control, cryptography, and

digital signatures, these measures are inadequate [5]. The ability to combine digital and physical assets is a hallmark of Cyber-Physical Systems (CPSs). Better scalability and flexibility than typical standalone systems are achieved by the integration of physical and cyber components, which allows for the expansion and reconfiguration of CPS [6]. The development of powerful and privacy-preserving ML-based defensive solutions has become imperative due to the rising complexity and frequency of assaults in distributed computing settings [7][8]. Despite their strength, traditional centralized learning models have serious flaws such data leaking, too directive communication, and weak spots. FL is a viable alternative that allows dispersed devices to train a collaborative model without transmitting initial data to a central server [9][10]. This decentralized model guarantees conformity with regulatory requirements, protects user privacy, and lessens systemic risk.

Federated Learning (FL) has shown great promise in dynamic and confined situations, such as underwater drone networks, where centralized learning is challenged by high latency and low bandwidth. AI, encompassing ML, DL, and NLP, has become a potent instrument for improving cloud security and privacy [11]. AI-driven frameworks provide automated incident response, real-time threat identification, and data processing that safeguards personal information, overcoming the drawbacks of conventional methods [12][13][14]. This study examines how AI may be used to create strong cloud security and privacy frameworks, assesses existing approaches, and suggests a scalable framework to counter modern threats. Additionally, the study highlights obstacles and suggests potential paths for improving AI-driven cloud security [15][16]. Although this likely offers multiple benefits, federated ML to cyber threat intelligence has a number of issues, such as communication overhead, heterogeneity of models, federated systems adversarial attacks, and scalability in large distributed settings [17]. These issues need to be addressed so that the cloud data infrastructures distributed globally can be effectively and safely detected when it comes to threats.

### *1.1 Significance of the Study*

This paper is important, as it suggests a proof of privacy-saving cyber threat detection model with Federated Learning combined with CNN model applied to cloud-based MIS systems. The technique allows joint threat detection on distributed systems without distributing unfiltered data, hence enhancing privacy and security of data. The proposed FL-CNN model is also the one that improves the detection accuracy and offers a scalable and efficient solution to the contemporary cloud cybersecurity systems. Contributions of the Paper The major contributions of the work are the following:

- It suggests an algorithmic cyber threat detection system that preserves privacy through FL-CNN.
- Processes the CIC-IDS-2017dataset using the preprocessing methods of missing value imputation, MinMax normalization, one-hot encoding, and attack label remapping.
- Deploys distributed model training to the multiple client nodes, which make sure that raw cybersecurity data is kept locally and that privacy is maintained.
- Shows the efficacy of federated learning in providing secure and scalable cyber threat intelligence in cloud-integrated MIS.

### *1.2 Justification and Novelty*

The justification for this study is the growing necessity for privacy-guaranteed cyber threat detection in cloud-integrated MIS contexts, where consolidated ML methods disclose confidential security information. The traditional models demand the exchange of raw data with a central server, which heightens the probability of data breach and loss of security. In response to this, this paper suggests a new combination of FL-CNN that can be used to train the model in a collaborative manner through distributed nodes without transfer of raw data. The approach enhances data privacy, scalability, and detectiveness, which is more appropriate in secure cyber threat intelligence in distributed cloud systems.

### *1.3 Structure of the Paper*

The rest of the paper is structured as follows: Section II examines relevant research on ML methods that protect privacy and cyber threat intelligence. The suggested technique, including dataset definition, data preparation, federated learning architecture, and model integration, is covered in Section III. Section IV showcases the outcomes of the experiments, assesses the performance, and compares it to current models. Finally, Section V summarizes the paper's weaknesses and future research prospects.

## 2. LITERATURE REVIEW

In this section, Table I provides a literature review of recent studies on Cyber Threat Intelligence in Global Cloud using ML and DL techniques. It provides a synopsis of the examined works' methodology, dataset, important results, limits, and possible future directions.

A. Mohamed et al. (2023) after preprocessing the data gathered from the network traffic, feature engineering techniques are used to extract the relevant characteristics. The results show that several ML algorithms can identify the many distinct kinds of attacks included in the UNSW-NB15 dataset. Various feature engineering methodologies and their effects on detection accuracy are also examined in the research [18].

In another study, A. Agarwal (2022) offered a unique method for detecting cyberattacks on load prediction data from the electrical grid. Using supervised ML algorithms, the second step is categorizing cyber threats. The last step is to use ensemble methods to construct a brand-new hybrid model. The novel strategy demonstrated an impressive 97.25% accuracy when tested on a publicly available dataset [19]. J. A. Abraham and V. R. Bindu (2021), an essential tool for information security, the IDS looks for unusual activity on a network using algorithms based on ML and DL. There has to be an 87% improvement in intrusion detection accuracy in order to raise detection rates while decreasing false alarms. Various ML classification algorithms' performance on the DARPAdataset is also compared in the research [20]. G. Yedukondalu et al. (2021) program has detected the rates of infiltration using the SVM and ANN algorithms. They check the data they requested for validity and abnormalities using each method. They used the NSL KDD dataset for this experiment. In conclusion, the SVM approach only managed 48% accuracy, whereas the ANN algorithm managed 97%. Therefore, compared to the SVM, the ANN model performs better on this dataset [21]. Likewise, D. Kapil et al. (2021) the regular and suspicious activity need to be classified using a rapid and effective approach. Additionally, a threat model spanning many networking levels is presented in this study. The findings for TPR, prec FPR, Fmeasure, and rec parameters are shown after conducting experimental analysis using the NSL_KDD dataset and the NB, RF, and J48 classification algorithms [22].

Table 1. Related Studies on Cyber Threat Intelligence In Cloud Performance Using Ml/Dl Techniques

| Author & Year | Methods | Dataset | Key Results | Limitations & Future Work |
|---|---|---|---|---|
| A. Mohamed et al. (2023) | Multiple Machine Learning algorithms with feature engineering | UNSW-NB15 dataset | Demonstrated effective detection of various attack types with improved detection accuracy through feature engineering | The work emphasizes feature engineering but lacks evaluation with advanced deep learning models. Future work could integrate deep learning and automated feature extraction methods. |
| A. Agarwal (2022) | Hybrid ensemble machine learning model | Public cyber attack dataset related to electric grid load prediction | Achieved accuracy of 97.25% for cyber attack detection | The model was tested on limited datasets and specific smart grid scenarios. Future work could extend the model for real-time smart grid monitoring and larger datasets. |

| | | | | |
|---|---|---|---|---|
| J. A. Abraham & V. R. Bindu (2021) | ML and DL algorithms for IDS | DARPA dataset | Achieved intrusion detection accuracy of 87% and improved detection rate with reduced false alarms | The approach is evaluated on older datasets such as DARPA, which may not represent modern attack patterns. Future work should consider modern datasets and real-time network environments. |
| G. Yedukondalu et al. (2021) | SVM and ANN | NSL-KDD dataset | ANN achieved 97% accuracy while SVM achieved 48% accuracy | The study compares only two algorithms and lacks broader algorithmic evaluation. Future work may include deep learning architectures and hybrid models for improved performance. |
| D. Kapil et al. (2021) | NB, RF, J48 classification algorithms | NSL-KDD dataset | Evaluated using TPR, Precision, FPR, F-measure, and Recall for classification of normal and suspicious activities | The work focuses mainly on traditional machine learning techniques. Future work could incorporate ensemble learning, deep learning, and testing on contemporary intrusion datasets. |

## 3. METHODOLOGY

Fig. 1 shows the FL workflow of the proposed CNN privacy-preserving framework of the work on detecting cyber threats. CIC-IDS-2017 data is used to start the process, and the next step is data preprocessing, which involves the use of missing values imputation, MinMax normalization, one-hot encoding, and attack label remapping. A division of the dataset into a training (80) and testing (20) sets is then done. Federated learning is then used whereby distributed client nodes are used to train the CNN model locally without transferring raw data. Acc, prec, rec, F1score and FPR are performance metrics that are used to evaluate the trained models. At last, the analysis, and comparison of the findings with current models are done to determine an efficacy of a suggested approach.

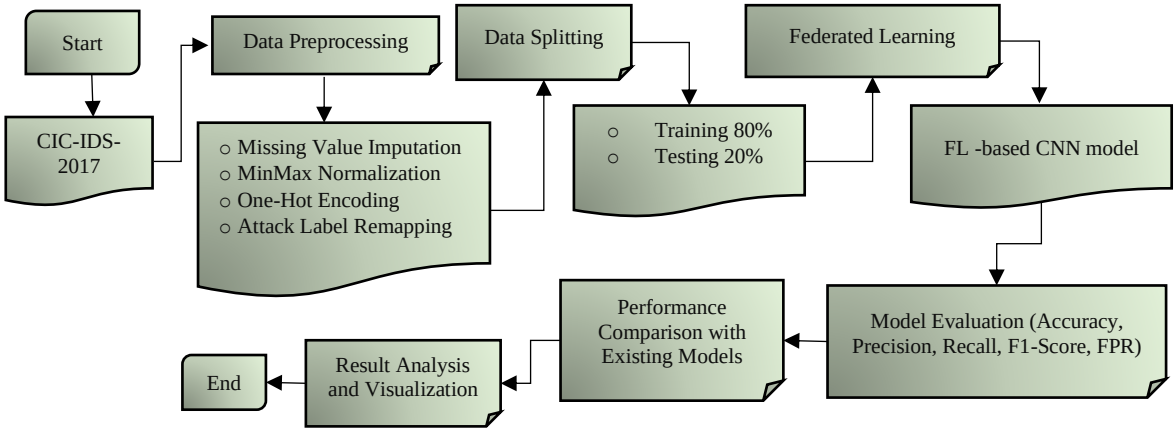


Figure1. Flowchart of the Proposed Federated Learning-based Privacy-Preserving Cyber Threat Detection.

The suggested methodology's subsequent phases are briefly discussed below:

### *4.1 Data Analysis and Visualization*

The utilized-CICIDS-2017 dataset represents real-time network traffic and contains both benign and malicious actions in the present day. The innocuous traffic includes the details of 25 people who utilize protocols including email, FTP, SSH, and HTTPS. Network data spanning five days is collected and dumped, with routine activity on some days and attacks on others.

BruteForceFTP, BruteForceSSH, "DoS," Heartbleed, WebAttack, Infiltration, Botnet, and "DDoS" are some of the several assaults that are injected. The CICIDS2017dataset was subjected to a comprehensive Exploratory Data Analysis (EDA).

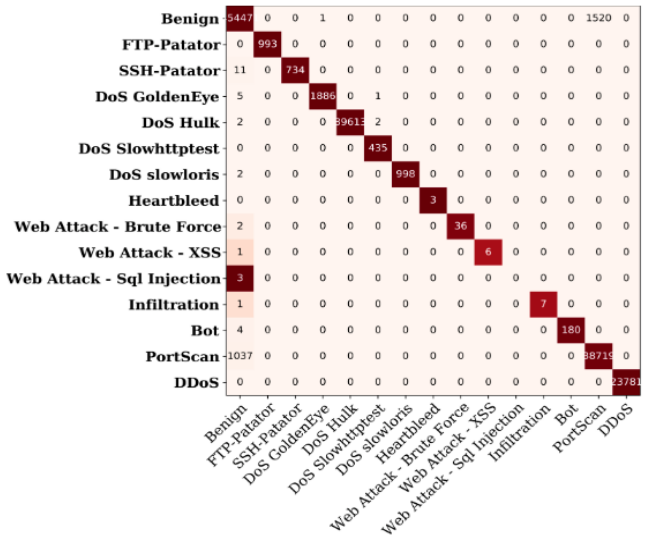


Figure 2. Correlation matrix of Dataset Features.

In Fig. 2 shows the correlation matrix of the relationship between all the various network traffic classes in the dataset, such as Benign, FTP-Patator, SSH-Patator, DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoS Slowloris, Heartbleed, WebAttack (BruteForce, XSS, SQL Injection), Infiltration, Bot, PortScan and DDoS. The diagonal values are highly correlated in the same category of the classification, which implies the dominance of proper classification, and the off-diagonal values reflect the small errors in classification between some types of attacks.

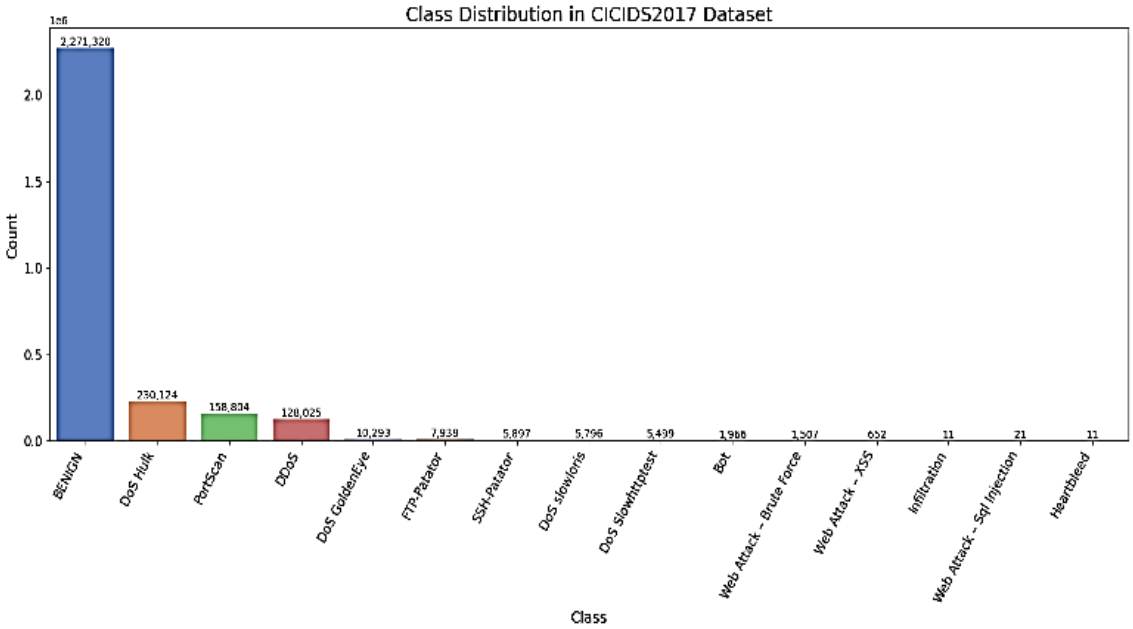


Figure 3. Class distribution in the CICIDS2017 dataset.

The distribution of various traffic classes in CICIDS2017 dataset. The samples belonging to the Benign class are the most numerous, whereas those that belong to attack classes include DoS Hulk, PortScan, DDoS, FTP-Patator and SSH-Patator that have relatively lower numbers of samples. Fig. 3 shows that there is a discrepancy between the dataset's classifications of legitimate traffic and various forms of cyberattacks.

### *4.2 Data Preprocessing*

Data cleansing, FeatureExtraction, normalization, and One-hotEncoding of categorical features are processes that are executed locally on each node as part of the preprocessing. Common techniques used in data preprocessing include:

- Missing value imputation: The purpose of feature-wise mean imputation is to guarantee that numerical features have full data while reducing distributional distortion by replacing any missing or null values.
- Feature scaling (MinMax normalization): MinMax normalization is employed to rescale all numerical features to the [0, 1] interval, thereby ensuring that all features have a uniform impact on the model during training and accelerating gradient convergence.
- One-hot encoding of categorical features: The use of One-hotEncoding to ConvertCategory variables (such protocol type or service) into BinaryVectors while maintaining non-ordinal associations allows for interoperability with neural network models.
- Attack label remapping for class balance: Class imbalance and improved generalizability of the classifier might be achieved by reclassifying the original AttackLabels by datasets (e.g., DoS, Probe, R2L, and U2R) into more generic categories [23].

### *4.3 Data Splitting*

An 80:20 split is used to construct a training set and a testing set from the preprocessed dataset. Model parameters are learned using the training set, and performance is assessed using the testing set.

### *4.4 Federated learning (FL)*

FL, a novel AI model developed by Google, performs better than traditional AI models. FL is a very effective machine learning paradigm that maintains data privacy across many decentralized edges while learning a range of input/output mapping functions. This function has the potential to close several knowledge gaps between traditional AI models and their power and energy system applications. In comparison to conventional ML models, FL is distinguished by its ability to process large-scale data, efficiently follow the data input/output mapping function, provide a generalizable model, and preserve data security and privacy. Additionally, it imposes a low computational burden during the training process. A central server gathers and compiles models from clients taking part in the learning process during centralized federated learning. On the server side, a common model is delivered down to the clients.

### *4.5 Integrating CNN with FL*

The proposed, privacy-conserving cyber threat detection in cloud-based uses a Federated Learning-based **CNN** model [24]. Within the scheme, various distributed client nodes train the CNN model on their own with their own cybersecurity data, including network traffic logs, system activity records, etc. CNN architecture consists of feature extraction Convolutional Lyers, ReLU activation functions, dimensionality reduction pooling layers, and fully connected layers of normal and malicious activity classification. Instead of transmitting the original data, each client transmits the parameters of the modified model to a central server. These changes are combined by the server using the FedAvg approach to create an improved global model, which is then delivered to each client for further training. This is a joint learning approach that improves threat detection performance, and ensures the data privacy in distributed cloud environments. The federated CNN model is trained using the AdamOptimizer with a LearningRate of 0.001 and a BatchSize of 32. The CNN architecture employs ReLU activation, 3×3 convolution kernels, 2×2 max-pooling layers, and a DropoutRate of 0.5 to prevent overfitting.

### *4.6 Evaluation Metrics*

A collection of common cybersecurity and ML measures are used to assess the suggested privacy-preserving FL framework [25]. These criteria were chosen

in order to do a thorough assessment of the model's functionality, communication effectiveness, and privacy protection among dispersed nodes in an IoT simulation.

3.6.1 Accuracy (ACC)

The overall accuracy of the model is measured by this statistic, which takes into account the proportion of samples that correctly forecast occurrences (both benign and malicious). The definition is given in Equation (1).

$$Accuracy = \frac{\mathrm{TN} + \mathrm{TP}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \quad (1)$$

This standardised measure is often used to evaluate FL-based IDS since it shows how reliable the model is in general for both benign and malicious categories.

3.6.2 Precision (PRE)

Precision is defined as the proportion of accurate predictions to the total number of positive forecasts. It shows the proportion of warnings that the system generates that are genuine threats. It is defined as Equation (2).

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

3.6.3 Recall (REC)

This shows the percentage of true positives that are accurately detected. It is derived as Equation (3).

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

3.6.4 F1 score

This balances both measures by taking the harmonic mean of prec and rec. It may be seen in Equation (4):

$$F1 = \frac{2*(precision*recall)}{precision+recall} \quad (4)$$

The F1 score provides a more fair assessment in situations with unequal class distributions by combining the advantages of both accuracy and recall. It often serves as the main performance indicator for federated intrusion detection.

3.6.5 False-Positive rate (FPR)

In contrast to the TPR, which indicates how well a model can identify dangers, the FPR shows how often data is incorrectly labelled as a different kind of threat. Equations (5) represent the FPR.

$$FPR = \frac{FP}{FP+TN} \quad (5)$$

The number of positively anticipated occurrences (i.e., instances when a security danger is present) is called TP (True positives). TN stands for "True Negatives," which are the number of times a negative occurrence (one in which a security concern is not present) is accurately anticipated. FP (False Positives) refers to the quantity of positive instances that were incorrectly predicted and The FN (False Negatives) is the number of unfavourable occurrences that were incorrectly predicted.

A standardised evaluation and reproducible results are guaranteed by the consistent application of these definitions across all experiments.

## 4. RESULT AND DISCUSSION

The experimental environment of this paper contains hardware and software environments, in which the hardware environment is Intel(R) Core(TM) i5-3230M, 2.6GHz, 12GB memory, Windows 10, and Python 3.6.5, Anaconda3. Table II compares the results obtained from the CIC-IDS-2017dataset using the suggested FL-based CNN model with the centralized CNN model. The findings reveal that the FL-based CNN can be more effective with the highest acc of 96.8, rec of 96.7, prec of 96.2, and F1score of 96.5 as opposed to the centralized model. There is also the FPR of the FL-based CNN is also 0.025, lower than 0.05 in the case of the centralized model, which implies better detection and less misclassification.

Table 2. Performance Metrics of CNN model integrated with FL on CIC-IDS-2017 Dataset

| Model | FL- based CNN | Centralized model |
|---|---|---|
| Accuracy | 96.8 | 94.3 |
| Precision | 96.2 | 92 |
| Recall | 96.7 | 92.3 |
| F1-score | 96.5 | 92.1 |
| FPR | 0.025 | 0.05 |

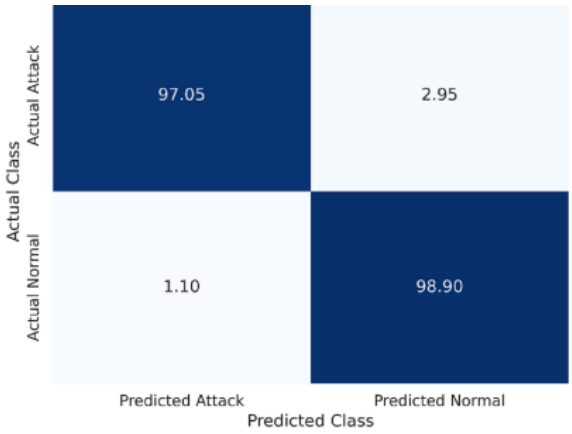


Figure 4. Confusion metrics of CNN Model.

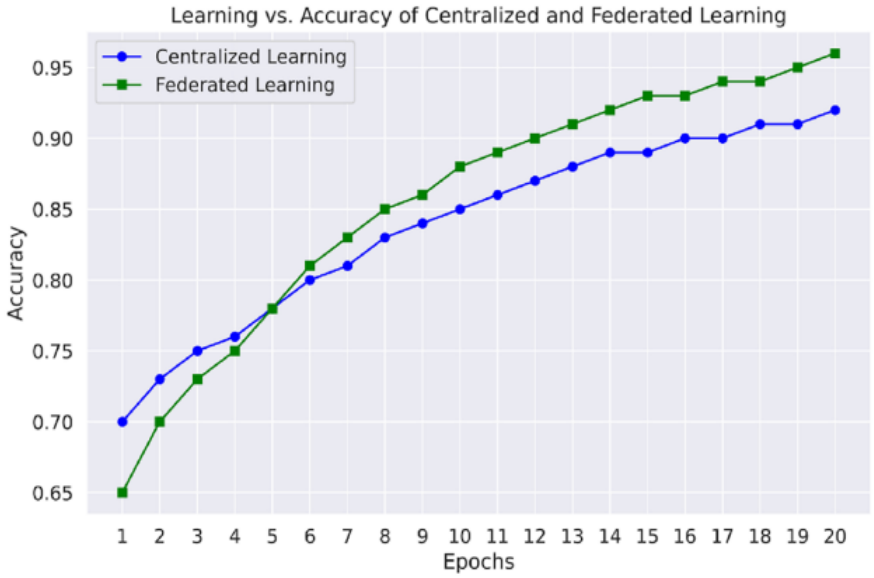


Figure 5. Learning vs. accuracy of centralized and FL of CNN

Fig. 4 displays the CNN model's classification results for both malicious and benign network traffic as measured by the confusion matrix. The metrics indicate that 97.05 of the attacks are rightly classified as attacks, and 2.95 are falsely classified as normal. Likewise, 98.90 of normal cases are also rightly detected with 1.10 of the cases categorized as attacks wrongly. Such findings reveal the efficacy of the CNN model in the detection of cyber threats with the least misclassification. Fig. 5 displayed the performance of the centralized CNN model and the FL-based CNN model in learning through several training epochs. The graph shows that as the number of epochs increases, both models gradually improve. Nevertheless, the FL-based CNN still attains greater accuracy than the centralized model when training is done in the initial stages. At the last epoch, the FL model about 96% accurate, and the centralized model would be about 92%, which proves that the federated learning improves the performance.

### *4.1 Comparison with Similar Works*

Table III displays the results of comparing the proposed FL-CNN model to several ML and DL models for cloud-based cyber threat detection while protecting user privacy. The findings indicate that the FL-CNN model has the most accurate results of 96.8, which are higher than the other models, including Naïve Bayes (86.71), Deep Multilayer Perceptron (91), SVM (92.27), Decision Tree (94.12), and RNN (94). These findings indicate that the performance of federated learning with CNN can be improved significantly in terms of threat detection and data privacy in the distributed cloud systems.

Table 3. Comparative Performance of Proposed and existing models for privacy preserving threat Threat in Cloud

| Model | Study | Accuracy |
|---|---|---|
| FL-CNN | Proposed | 96.8 |
| Naïve Bayes | [26] | 86.71 |
| DMLP | [27] | 91 |
| SVM | [28] | 92.27 |
| DT | [29] | 94.12 |
| RNN | [30] | 94 |

### *4.2 Limitations of the Study*

The suggested methodology is somewhat limited in terms of the diversity of datasets, communication cost in federated learning, and the application of one deep learning model.

- The suggested model is tested only with the CIC-IDS-2017dataset which might be insufficient to help encapsulate all the actual cyber threats.
- Federated learning adds overhead with regards to communication because of frequent sharing of parameters between client nodes and the central server.
- The framework states that the participation of clients is stable, whereas client dropout or shaky network conditions can influence the training process.
- The research only employs CNN architecture, and does not investigate other superior deep learning models.
- This work does not take possible adversarial or poisoning attacks in federated learning settings into account.

### *4.3 Future Research Directions*

It is possible to improve the proposed framework through future work to ensure increased scalability, security and improved model performance in distributed clouds.

- Future research can assess the model on several and more timely cybersecurity data sets so it can be more generalized.
- Federated learning can be combined with more complex models like Transformers, LSTM, and hybrid deep learning models.
- Data security may be improved by using privacy-enhancing strategies like safe aggregation and differential privacy.
- In federated learning, overheads in computational and network resources can be minimized through the enhancement of the efficiency of communication.
- The framework can be scaled to real-time cyber threats detection in big-scale cloud and IoT.

## 5. Conclusion

The faster implementation of cloud-integrated Management Information Systems (MIS) has exposed the organization to an array of dangerous computer threats that include ransomware, DDoS attacks, and APTs. This paper suggested a privacy-preserving cyber threat detection system based on FL-CNN in cloud-based Management Information System settings. This technique reduces the dangers associated with having a central data store and maintains data privacy by letting dispersed client nodes train the models locally and transmitting just a model parameter. The model is trained using the CIC-IDS-2017dataset, with the use of the preprocessing methods that included missing value imputation, Min-Max normalization, one-hot encoding, and attack label remapping. Experiments proved that the proposed FL-CNN model is better with 96.8% acc, 96.2% prec, 96.7% rec, and 96.5% F1score, and false positive rate 0.025, than the centralized CNN model, as well as some of the existing methods, including Naive Bayes, DMLP, SVM, Decision Tree, and RNN. The findings show that federated learning and CNN work together to make dispersed cloud data more secure and improve cyber threat detection accuracy.

## REFERENCES

[1] M. Jouini and L. B. A. Rabai, "A Security Framework for Secure Cloud Computing Environments," *Int. J. Cloud Appl. Comput.*, vol. 6, no. 3, pp. 32–44, Jul. 2016, doi: 10.4018/IJCAC.2016070103.

[2] A. Gupta, "What Is The Right Security Posture? A Perspective on Cloud Computing Security Threats and Risk Assessment," *Int. J. Emerg. Res. Eng. Technol.*, vol. 4, no. 4, 2023, doi: 10.63282/3050-922X.IJERET-V4I4P112.

[3] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "DDoS Attack Detection Using Machine Learning Techniques in Cloud Computing Environments," in *2017 3rd International Conference of Cloud Computing Technologies and Applications*

*(CloudTech)*, IEEE, Oct. 2017, pp. 1–7. doi: 10.1109/CloudTech.2017.8284731.

[4] S. K. Chintagunta and S. Amrale, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *TIJER--Int. Res. J*, vol. 9, no. 10, pp. 49–55, 2022.

[5] V. K. Sharma, "Security and Threat Mitigation in 5G Core and RAN Networks," *Int. J. Multidiscip. Res.*, vol. 3, no. 5, pp. 1–10, 2021.

[6] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019.

[7] S. Singamsetty, "Edge Nexus: Bridging AI and Data Engineering for Seamless Edge Computing," *Turkish Online J. Qual. Inq.*, vol. 13, no. 1, pp. 2343–2351, Mar. 2022, doi: 10.53555/axxezz36.

[8] G. Sarraf, "BalanceNet: Addressing Class Imbalance in AI-Powered Intrusion Detection Through Adaptive Sampling," *Asian J. Comput. Sci. Eng.*, vol. 8, no. 4, pp. 1–8, 2023, doi: 10.22377/ajcse.v8i04.268.

[9] M. Lane, A. Shrestha, and O. Ali, "Managing the Risks of Data Security and Privacy in the Cloud: A Shared Responsibility between the Cloud Service Provider and the Client Organisation," *Bright Internet Glob. Summit*, 2017.

[10] A. Parupalli and H. Kali, "An In-Depth Review of Cost Optimization Tactics in Multi-Cloud Frameworks," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 5, pp. 1043–1052, Jun. 2023, doi: 10.48175/IJARSCT-11937Q.

[11] O. Achbarou, "A New Distributed Intrusion Detection System Based on Multi-Agent System for Cloud Environment," *Int. J. Commun. Networks Inf. Secur.*, vol. 10, no. 3, Apr. 2022, doi: 10.17762/ijcnis.v10i3.3546.

[12] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3118642.

[13] V. K. Sharma, "AI-Based Anomaly Detection for 5G Core and RAN Components," *Int. J. Sci. Res. Eng. Manag.*, vol. 6, no. 1, pp. 1–6, 2022.

[14] S. Amrale, "Proactive Resource Utilization Prediction for Scalable Cloud Systems with Machine Learning," *Int. J. Res. Anal. Rev.*, vol. 10, no. 4, pp. 758–764, 2023.

[15] M. Hafsa and F. Jemili, "Comparative Study Between Big Data Analysis Techniques in Intrusion Detection," *Big Data Cogn. Comput.*, vol. 3, no. 1, Dec. 2018, doi: 10.3390/bdcc3010001.

[16] C. Tayal, "Designing Hybrid ETL Pipelines for Multi-Cloud Integration," *Int. J. Emerg. Trends Comput. Sci. Inf. Technol.*, vol. 4, no. 4, pp. 129–134, 2023, doi: 10.63282/3050-9246.IJETCSIT-V4I4P114.

[17] R. Patel, "Advancements in Renewable Energy Utilization for Sustainable Cloud Data Centers : A Survey of Emerging Approaches," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 5, pp. 447–454, 2023.

[18] A. Mohamed, J. Heilala, and N. S. Madonsela, "Machine Learning-Based Intrusion Detection Systems for Enhancing Cybersecurity," in *2023 Second International Conference on Smart Technologies for Smart Nation (SmartTechCon)*, IEEE, Aug. 2023, pp. 366–370. doi: 10.1109/SmartTechCon57526.2023.10391626.

[19] A. Agarwal, "Load forecast anomaly detection under cyber attacks using a novel approach," in *Proceedings of 4th International Conference on Cybernetics, Cognition and Machine Learning Applications, ICCCMLA 2022*, 2022. doi: 10.1109/ICCCMLA56841.2022.9988990.

[20] J. A. Abraham and V. R. Bindu, "Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review," in *2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, 2021, pp. 1–4. doi: 10.1109/ICAECA52838.2021.9675595.

[21] G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh, and A. Saiteja, "Intrusion Detection System Framework Using Machine Learning," in *Proceedings of the 3rd International Conference on Inventive Research in Computing Applications, ICIRCA 2021*, 2021. doi: 10.1109/ICIRCA51532.2021.9544717.

[22] D. Kapil, N. Mehra, A. Gupta, S. Maurya, and A. Sharma, "Network Security: Threat Model, Attacks, and IDS Using Machine Learning," in *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, IEEE, Mar. 2021, pp. 203–208. doi: 10.1109/ICAIS50930.2021.9395884.

[23] S. Chatterjee, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," *Int. J. Multidiscip. Res.*, vol. 3, no. 4, pp. 1–10, Aug. 2021, doi: 10.36948/ijfmr.2021.v03i04.34396.

[24] H.-N. Nguyen, H.-T. Nguyen, D. Lescos, and Q. Nhat, "Classification of ransomware attacks using federated learning based on the CNN model," in *Annual conference of Vietnamese young scientists*, 2022.

[25] G. Sarraf, "Autonomous Ransomware Forensics: Advanced ML Techniques for Attack Attribution and Recovery," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1377–1390, Jul. 2023, doi: 10.48175/IJARSCT-11978W.

[26] S. S. Panwar, P. S. Negi, and Y. P. Raiwani, "Implementation of Machine Learning Algorithms on CICIDS-2017 Dataset for Intrusion Detection using WEKA," *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, Sep. 2019, doi: 10.35940/ijrte.C4587.098319.

[27] S. Ustebay, Z. Turgut, and M. A. Aydin, "Intrusion Detection System with Recursive Feature Elimination by Using Random Forest and Deep Learning Classifier," in *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings*, 2019. doi: 10.1109/IBIGDELFT.2018.8625318.

[28] P. Verma, J. G. Breslin, and D. O'Shea, "FLDID: Federated Learning Enabled Deep Intrusion Detection in Smart Manufacturing Industries," *Sensors*, vol. 22, no. 22, p. 8974, Nov. 2022, doi: 10.3390/s22228974.

[29] S. Mishra, A. Albarakati, and S. K. Sharma, "Cyber Threat Intelligence for IoT Using Machine Learning," *Processes*, vol. 10, no. 12, p. 2673, Dec. 2022, doi: 10.3390/pr10122673.

[30] M. M. Rashid, S. U. Khan, F. Eusufzai, M. A. Redwan, S. R. Sabuj, and M. Elsharief, "A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks," *Network*, vol. 3, no. 1, pp. 158–179, Jan. 2023, doi: 10.3390/network3010008.