International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group | Volume 7 Issue 1 PP 238-245, 2026
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V7I1P130

Original Article

Development of a Generative AI-Assisted Network IDS for Intelligent Cloud Cybersecurity Monitoring

Dr. Prathviraj Singh Rathore
Assistant Professor, Department of Computer Sciences and Applications, Mandsaur University, Mandsaur.

Received On: 17/01/2025 ***Revised On: 18/02/2026*** ***Accepted On: 21/02/2026*** ***Published On: 24/02/2026***

Abstract *- In the cloud security paradigm, threat detection and response exhibit structural and functional symmetry, where each detected threat triggers a corresponding automated or manual response. Cloud security is critical due to the increasing reliance on cloud computing to store, process, and transmit sensitive data across various sectors. In order to resist insider threats and external attacks to cloud systems, the present study examines features of DDoS attacks detection and classification based on CICDDoS2019 data set consisting of 88 features and millions of records. Preprocessing was done to eliminate categorical and duplicate features, deal with infinite values, label encoding and min-max normalization. Principal Component Analysis (PCA) was used to select features and therefore dimensionality was maintained by including vital information. An effective model of complex data was acquired by training a Variational Autoencoder (VAE) model (made up of an encoder and decoder) to maximize the evidence lower bound (ELBO). The model had 99.79% accuracy, 98.57% precision, 98.55% recall and 98.56% F1-score, which was better than classical machine learning methods such as RNN, Kalman Backpropagation Neural Networks, and Logistic Regression proving good, dependable, and efficient cloud-based cybersecurity threat detection.*

Keywords *- Intrusion Detection and Protection System, Event Monitoring, Networking, Artificial Intelligence, Principal Component Analysis (PCA), Internet of Things (Iot).*

1. Introduction

Data security and integrity have become critical concerns in the era of cloud computing (CC) [1][2] and digital transformation. Although cloud platforms provide scalability, flexibility, and cost efficiency, sensitive information stored in cloud environments is highly vulnerable to cyberattacks [3], data breaches [4], and unauthorized access [5]. The rapid integration of cloud services with emerging technologies such as the Internet of Vehicles (IoV) and Industrial Internet of Things (IIoT) has further increased the attack surface [6]. These interconnected ecosystems generate massive volumes of real-time data [7], making intelligent and automated cybersecurity mechanisms essential for secure cloud information retention [8][9].

The IoV extends IoT capabilities by connecting vehicles, users, sensors, and cloud infrastructure [10][11] to enhance transportation efficiency and user experience. Similarly, IIoT environments rely on interconnected edge devices and cloud-based platforms [12][13] to support smart manufacturing and industrial automation [14][15][16]. However, such distributed and dynamic systems are highly susceptible to anomalies, malware, and sophisticated cyber intrusions [17]. Real-time stream processing and autonomous computing are therefore required to predict system failures and security breaches at early stages [18], enabling proactive mitigation before critical damage occurs [19][20].

Intrusion Detection Systems (IDS) are widely adopted to monitor malicious activities within cloud [21] and IoT networks. IDS can be categorized into Host-Based IDS (HIDS) and Network-Based IDS (NIDS) [22], each designed to monitor host-level events or network traffic, respectively [23][24][25]. Although machine learning (ML) and deep learning (DL) techniques have enhanced IDS performance, existing approaches still suffer from high false positive rates, limited adaptability to evolving threats [26], computational inefficiencies, and scalability challenges in large-scale cloud-IoV environments. Traditional centralized architectures often fail to effectively capture complex sequential attack patterns in real-time scenarios [27][28][29].

To overcome these limitations, this research focuses on the Development of a Generative AI-Assisted Network IDS for Intelligent Cloud Cybersecurity Monitoring. By integrating generative AI with advanced deep learning models, the proposed framework enhances anomaly detection accuracy, improves adaptability to emerging attack strategies, and reduces false alarms. The generative component enables dynamic threat modelling and synthetic attack pattern generation, strengthening real-time monitoring and proactive defense mechanisms. This approach provides a scalable, intelligent, and resilient solution for next-generation cloud cybersecurity environments [30][31][32][33].

1.1. Motivation and Contribution

The research is inspired by the fact that security issues in cloud systems continue to escalate, particularly in complex systems such as the IoV and IIoT, in which sensitive information is at risk due to cyberattacks. Traditional machine learning and IDS control mechanisms find it hard to

deal with dynamic and high volume of data. The study will focus on creating a generative AI-supported network IDS that will lead to better anomaly detection, low false alarms, and a scalable, intelligent, and resilient cloud cybersecurity solution. This research offers several key contributions as listed below:

- The dataset used to carry out comprehensive cloud cybersecurity monitoring and detection of DDoS attacks was the CICDDoS2019 dataset.
- Systematically preprocessed data such as cleaning, normalization, encoding labels and dimensionality reduction by PCA to improve the quality of data.
- Normalized the tables and selected features to maximize the performance, lessen redundancy and select the most relevant attributes.
- Designed a Variational Autoencoder (VAE) that is effective to detect and classify DDoS attacks in the cloud environment.
- Outperformed with high accuracy, precision, recalling, and F1-score that indicates the strength and reliability of the proposed solution in monitoring cloud cybersecurity.

1.2. Novelty and Justification

This study is novel considering that it combines exhaustive data preprocessing and feature optimization using PCA with a deep learning model to generate clouds intrusion detectors. The model is able to capture underlying traffic patterns and identify anomalous behavior using the power of a Variational Autoencoder (VAE) which is more resilient to complex and unseen cyber-attacks. Systematic feature selection is better in computational efficiency and does not reduce the ability to detect features. Such a solution can be explained by the rising complexity of attacks in the clouds, which demand adaptive, scaling, and intelligent detection systems that cannot be addressed with the help of conventional machine learning methods.

1.3. Organization of the Paper

The flow of the study is the following one: Section II is the literature review on cloud cybersecurity and DDoS detection. Section III explains the CICDDoS2019 dataset, preprocessing, feature selection and proposed VAE model. Section IV provides the findings and comparison of the experiments. Section V provides the conclusion and recommendations of future research.

2. Literature Review

This study was informed by a thorough review and analysis of the major research studies performed on the topic of Cloud Cybersecurity Monitoring, which will help to improve the development of this study.

Yesuraju *et al.* (2025) determine the effects of intrusion detection in a distributed environment using many nodes. Stacked ensembles models performed best with a given accuracy score of 96.3%, and FL model was also performing comparatively well with an accuracy score of 94.5%. The results reveal that federated approaches coupled with ensemble approaches can eventually achieve scalability, accuracy, and privacy-preserving IDS solutions which have practical potentials of application in IoT, industry, and multi-organizational networks[34].

Venkatesh *et al.* (2025) benchmark intrusion detection data sets NSL-KDD and CICIDS2017, the system is evaluated to be 97.8 accurate, outperforming existing centralized and federated models in both communication overhead and detection latency. The method shows that real-time cyber threat intelligence can be addressed with a scalable, secure and robust solution with potential protective implications to both enterprises and critical infrastructures[35].

Jyothi *et al.* (2024) classified using a number of deep learning and machine learning techniques for both binary and multi-class purposes. test the suggested intelligent model on the ToN_ IoT dataset to see how well it performs. With the suggested method, were able to achieve a 99.98% accuracy rate and a lowered error rate of 0.016% for multi-class classification, and a 0.001 % reduction in the error rate for binary classification[36].

Tocci, Zhou and Zhang (2023) implementations train the network in this application, but do not take advantage of the hardware such as FPGA. After training, the agent can effectively identify between benign traffic, DDoS attacks, and port scan attacks with an accuracy of over 90%, running inference at a speed of 51.3 frames-per-second (FPS) on a AMD Ryzen 5600x CPU. Through the use of Vitis-AI, the neural network achieved 5886.85 FPS with no accuracy loss on the Xilinx Zynq UltraScale+ ZCU102 FPGA, providing a 100× increase in performance. This demonstrates the benefit of hardware acceleration when in deployed intrusion detection systems[37].

Divakar *et al.* (2021) measured in terms of correct analysis of the network traffic as normal or abnormal and the time taken to detect it. As per the observed results the proposed IDS system is providing the best results for XGB model which gives 95.57 % of accuracy and the time taken to do it is come out as 3.03 seconds. The entire experiment is executed both in Central Processing Unit (CPU) and Graphical Processing UnitGPU) environment and a comparative analysis is done in terms of execution time[38].

Patel, Choe and Halabi, (2020) explore a gradient boosting decision tree, especially LightGBM, which is a relatively new and powerful method, to predict future malware attacks on cloud computing systems. they use a large and sparse dataset provided by Microsoft and show that approach is suitable for predicting malware attacks using large datasets with 73.89% accuracy compared to conventional machine learning methods[39].

Saad *et al.* (2019) Proposed Bidirectional long short-term memory (BLSTM) is used to detect incidents over unified threat management (UTM) platform operated on cloud network. Results are compared with K-nearest neighbor which is a baseline technique. Time series input

samples recorded over UTM platform are used for training and testing purposes. They obtain accuracy score of 98.47% with 0.0186 mean squared error (MSE) using KNN while BLSTM provides 98.6% accuracy score with 0.002 loss, which is better than the KNN[40].

In Table 1, the recent studies on Cloud Cybersecurity Monitoring overview, the proposed models, datasets used, key findings, and all challenges that were addressed.

Table 1: Recent Studies on Cloud Cybersecurity Monitoring for Cybersecurity

Author	Proposed Work	Results	Key Findings	Limitations & Future Work
Yesuraju et al., (2025)	Federated Learning (FL) with stacked ensemble models for distributed intrusion detection	96.3% accuracy (Stacked Ensemble), 94.5% accuracy (FL)	Federated + ensemble approaches improve scalability, privacy preservation, and IDS accuracy in distributed IoT and industrial networks	Needs further real-world large-scale deployment validation and optimization of communication overhead
Venkatesh et al., (2025)	Benchmarking IDS using NSL-KDD and CICIDS2017 with improved federated approach	97.8% accuracy	Outperforms centralized and federated models in communication overhead and detection latency; scalable real-time threat intelligence	Requires evaluation on more diverse real-time datasets and adversarial scenarios
Jyothi et al., (2024)	Intelligent DL/ML-based IDS evaluated on ToN_IoT dataset	99.98% accuracy (multi-class), 0.016% error; 0.001% error reduction (binary)	High-precision detection for both binary and multi-class classification	Possible overfitting risk; requires validation on other heterogeneous datasets
Tocci, Zhou & Zhang (2023)	Hardware-accelerated IDS using FPGA (Vitis-AI)	>90% accuracy; 51.3 FPS (CPU); 5886.85 FPS (FPGA)	100× performance improvement with FPGA without accuracy loss; suitable for real-time IDS	Focused mainly on DDoS and port scan; expansion to other attack types needed
Divakar et al., (2021)	XGBoost-based IDS evaluated on CPU and GPU	95.57% accuracy; 3.03 seconds detection time	GPU improves execution time; XGB performs best among tested models	Limited dataset diversity; scalability testing required
Patel, Choe & Halabi (2020)	LightGBM-based malware attack prediction in cloud	73.89% accuracy	Suitable for large and sparse datasets; efficient malware prediction	Moderate accuracy; improvement possible with hybrid or deep learning models
Saad et al., (2019)	BLSTM-based IDS on cloud UTM platform compared with KNN	98.6% accuracy (BLSTM); 98.47% (KNN)	BLSTM outperforms KNN with lower loss; effective for time-series intrusion detection	Needs testing under large-scale cloud deployments and diverse cyber threats

Research gaps: In spite of the fact that the existing studies have been shown to be highly accurate in terms of intrusion detection based on federated learning, ensemble models, deep learning and hardware acceleration, there are a number of research gaps. The strategies of most are based on optimizing accuracy, paying minimal attention to real-time flexibility, dynamic evolution of attacks, and cross-dataset genericity. Also, most models are tested on certain benchmark datasets and it is questioned how these models would be able to scale and perform well in uncertain cloud and IoT settings. Thus, it is necessary to have a cohesive, light, and flexible IDS architecture that guarantees high accuracy, low latency, communication overhead, and high level of privacy in large scale distributed systems.

3. Research Methodology

The offered methodology employed the CICDDoS2019 dataset, where the initial stages of data preprocessing (removal of categorical and duplicate variables and working with infinite values) and analysis were conducted. This is followed by label encoding of the data, normalization, as MinMax scaling and optimization of the features based on PCA. Having divided into training and testing set, a Variational Autoencoder (VAE) intrusion detector model is applied. Lastly, the model performance is measured with the help of common measures such as accuracy, precision, recall, and F1-score. Figure 1 below depicts the proposed Network IDS flow chart of Intelligent Cloud Cybersecurity Monitoring.

A description of every step included in the proposed methodology is presented in the following section:

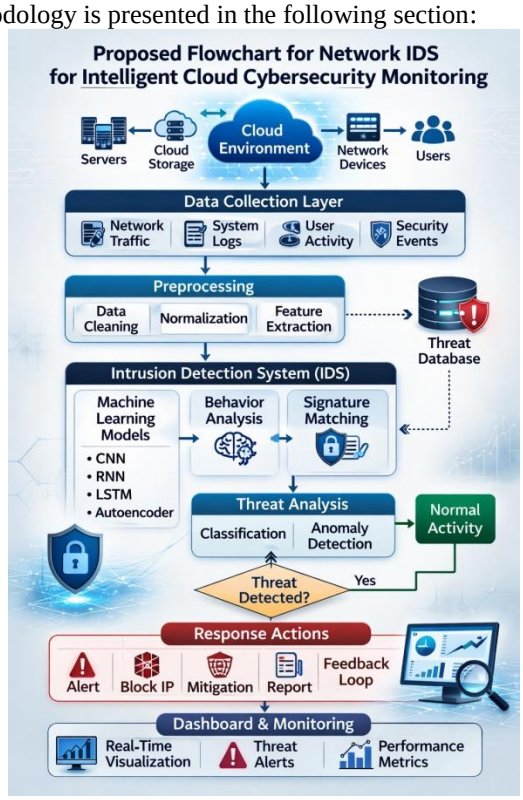

Fig 1: Proposed Flowchart for Network IDS for Intelligent Cloud Cybersecurity Monitoring

3.1. Data Gathering and Analysis

The present study makes use of CICDDoS2019 dataset sourced from Kaggle. The CICDDoS2019 data is 88-featured with millions of records. The dataset has 51- normal records and 49- attacks. The data will include the latest, common, and benign attacks of DDoS. The information on the spread of attacks, feature-correlation and so forth was visualized in the form of bar plots and heatmaps, which are provided below:

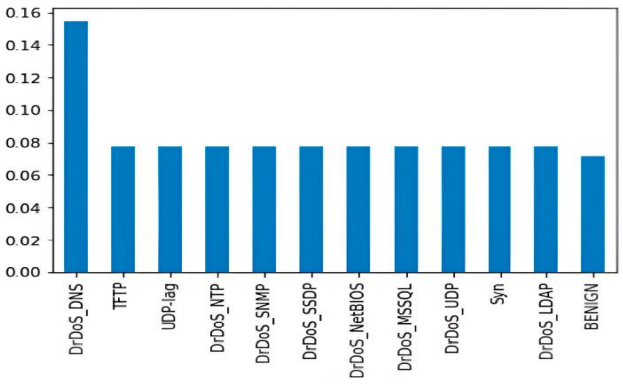

Fig 2: Bar Graph of Class Distribution of the CICDDOS2019 Dataset

Figure 2 indicates the distribution of classes of the dataset, with the majority of the classes being relatively balanced, with one of them having a small percentage more than the others.

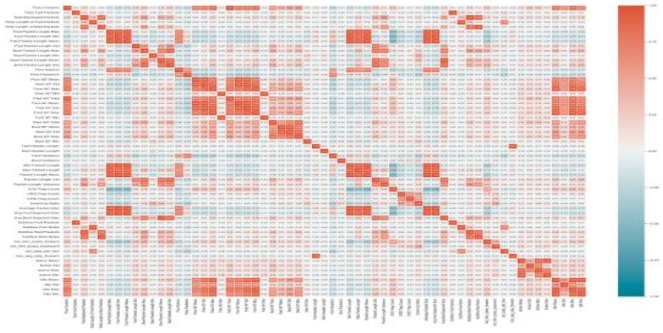

Fig 3: Correlation Matrix Heatmap on CICDDOS2019 Dataset for Cloud Cybersecurity Monitoring

The correlation heatmap of the dataset features is presented in figure 3. Strong positive correlations are present in the plot along the diagonal and between a few groups of features, which have related or dependent attributes, but the rest of the features do not exhibit strong correlations. This analysis is useful in determining the relationship of features and possible redundancy of the data set.

3.2. Data Pre-processing

The data preparation involved the use of CICDDOS2019 data set and the processing of the data set in several steps in a structured way. The procedure entailed data files concatenation, data cleaning encompassing categorical attributes, duplicate features, replacing the infinite values, and label encoding of the data which were to be used in modelling. These initial methods of preprocessing allowed a clean and consistent dataset to be obtained in a machine-readable format to be effectively analyzed.

The key preprocessing processes can be summarised as follows:

- Remove categorical data: Preprocessing eliminated categorical data so that they could be compatible with machine learning algorithms that use numbers. This will aid in enhancing the model efficiency and will also avoid mistakes that can be created due to the non-numeric input features.
- Remove duplicated features: In preprocessing, duplicated features were eliminated to eliminate redundancy in the dataset. The step helps to eliminate redundant complexity, increase the efficiency of computations, and improve the overall performance of the model.
- Replace infinities: During preprocessing, the infinite values were substituted because it is needed to ensure consistency of the data and avoid the occurrence of computational errors when training the model. It is a step that enhances numerical stability and better reliability in the learning process.
- Label Encoding: Label encoding has been used to change categorical class labels into numerical representation so that they can be compatible with the model. This conversion will allow machine learning algorithms to work with categorical outputs better and enhance the computational efficiency.

3.3. Min-Max Normalization

Data normalization is the procedure that is performed to ensure consistency of the data in all the fields and entries. The method that uses in constructing the model is min-max normalization which transforms the data to a range of 0 to 1. The min-max normalization is employed to normalize the values of the various characteristics in the CICDDOS2019 dataset to a fixed range. Subsequently, the NaNs are treated like missing values, which are ignored in fit, and stored in transform.

$$X_{normalized} = \frac{X - X_{minimum}}{X_{maximum} - X_{miimum}} \dots\dots (1)$$

3.4. Feature selection using PCA

One of the most critical machine learning processes is feature selection, which entails the process of establishing the most pertinent input variables in the training of a model. It assists in the dimensionality reduction, elimination of the redundant or irrelevant data, and the enhancement of the computational efficiency. In choosing features that are significant, the model learns more effectively and it takes less time to train and generalizes better. The Principal Component Analysis (PCA) method is used to select a set of features (that is, reduce the number of correlated variables) into fewer uncorrelated principal components that give up the majority of the variance of the data. The best principal components are chosen and thus dimensionality reduction is achieved and crucial information is retained to enhance model efficiency and performance.

3.5. Data Splitting

The split of the train and test set was done in a stratified manner. The dataset has been preprocessed to suit the developed model. The obtained dataset is further split into 70% training set and 30% testing set.

3.6. Classified Model: Variational Autoencoder (VAE)

In this section, we provide a description of Variational AutoEncoder (VAE). Our proposed method is based on these models.

Variational AutoEncoder [41] is a deep latent generative model $p_\theta(x,z) = p_\theta(x|z)p(z)$ consisting of an inference model $q_\phi(z|x)$ (encoder) and a generative model $p_\theta(x|z)$ (decoder). VAE approximates the posterior $p_\theta(z|x)$ by the inference model as shown in equation (1):

$$p_\theta(z|x) \approx q_\phi(z|x) \dots (1)$$

VAE optimizes the variational lower bound (ELBO) of the marginal log-likelihood of data given in equation (2):

$$\mathcal{L}_{\theta,\phi}(x) = \log p_\theta(x) - D_{KL}(q_\phi(z|x)||p_\theta(z|x)) \dots (2)$$

Both inference and generative network of VAE are jointly trained to maximize the ELBO. VAE amortizes variational inference (VI) by the encoder network. VAE uses fully-factorized Gaussian as the posterior distribution [42]. However, fully-factorized Gaussian does not have enough expressive power and cannot properly capture complex posterior distribution [43]. This causes approximation error. Another problem of VAE is the amortization error that causes due to amortized inference of posterior distribution.

4. Performance and Result Discussion

This experiment was performed on a system with a 2.3 GHz 8-core 9 th -generation Intel Core i9 processor (Turbo Boost up to 4.8 GHz), 16 GB of DDR4 RAM, and AMD Radeon Pro 5500M graphics card, with 4 GB of GDDR6 memory. It had 1 TB SSD, 16-inch Retina display (3072 x 1920 resolution), and ports consisted of four Thunderbolt 3 (USB-C) ports, a headphone jack, and SDXC card reader.

4.1. Evaluation Metrics

Several standard measures were used to determine the performance of the proposed model. First, a confusion matrix was created to show the results in the classification by showing the number of correct and incorrect predictions of each class. Based on this matrix the values of True Positives (TP), False Positives (FP), True Negatives (TN) and False Negatives (FN) were derived. Through these values, important evaluation metrics were calculated including accuracy, precision and recall and F1-score as mentioned below:

Accuracy: The ratio of the number of instances correctly predicted by the trained model to the total number of instances in the dataset (input samples). It is given as (3):

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{Fp} + \mathrm{TN} + \mathrm{FN}} \dots . (3)$$

Precision: Precision is the proportion of positive instances successfully predicted to all positive instances predicted by the model. Precision indicates. How good the classifier is in predicting the positive classes is expressed as (4):

$$Precision = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \dots . (4)$$

Recall: This metric, the ratio of events that were accurately predicted as positive to all instances that should have proved positive. In mathematical form it is given as (5):

$$Recall = \frac{\mathrm{TP}}{TP + FN} \dots\dots . (5)$$

F1 score: It is a combination of the harmonic meaning of precision and recall, that is, it helps to balance recall and precision. Its range is [0, 1]. Mathematically, it is given as (6):

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \dots\dots . (6)$$

4.2. Result Analysis

The proposed VAE model was trained on the CICDDoS2019 dataset and tested on the basis of the key performance indicators, including accuracy, precision, recall, and F1-score, summarized in Table II. This model was entirely accurate (99.79), precise (98.57), recalls (98.55) and its F1-score was 98.56 which is a good and balanced capability of classification. Such results demonstrate that the suggested VAE model is robust and sound in vulnerability to identify and prevent cyber threats in the cloud.

Table 2: Model Performance Network IDS for Intelligent Cloud Cybersecurity Monitoring

Matrix	Variational Autoencoder (VAE)
Accuracy	99.79
Precision	98.57
Recall	98.55
F1-score	98.56

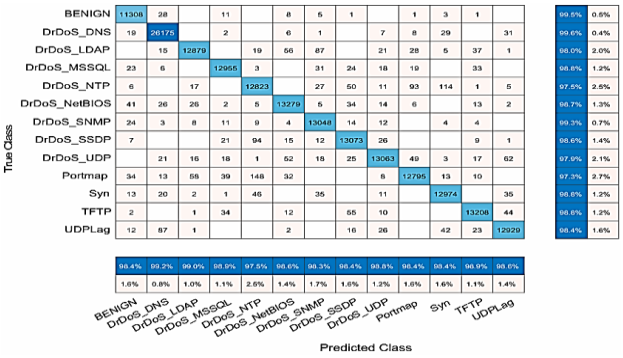

Fig 4: Confusion Matrix for VAE Model

The confusion matrix (Figure 4) of 13 classes has high values on the diagonal which represents a high rate of correct classification (9799) and a low rate of misclassification, which proves to be highly successful overall in the model.

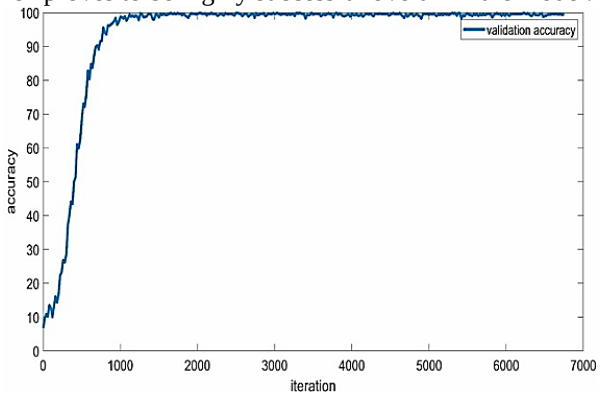

Fig 5: Accuracy Curve for VAE Model

Figure 5 demonstrates the validation accuracy against training iterations, and there is fast increase to 99.7 percent during the initial 1000 iterations, and thereafter, there is no significant increase in the performance, which means good convergence.

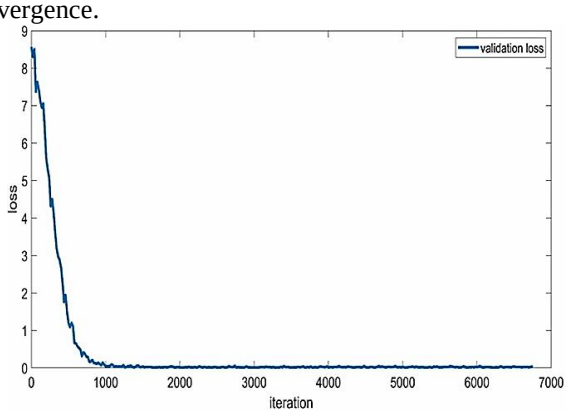

Fig 6: Loss Curve for VAE Model

Figure 6 indicates that validation loss is declining fast to almost a zero value in the initial 1000 iterations and it is kept constant thereafter, which is a good sign of convergence and successful learning.

4.3. Comparative analysis

Table III compares the performance of various ML and DL models of Network IDS of Intelligent Cloud Cybersecurity Monitoring. Compared to the traditional models like RNN, Kalman Backpropagation NN, and Logistic Regression, which have an accuracy of between 93% and 95% respectively, the proposed VAE model has 99.79% accuracy and balanced precision, recall and F1-score (98.5%), which is much higher, and they can detect much better.

Table 3: Comparison of Different ML and DL Models for Network IDS for Intelligent Cloud Cybersecurity Monitoring

Model	Acc.	Pre.	Rec.	F1-sc.
RNN[44]	93.49	96.25	98.95	97.58
Kalman back Propagation NN[45]	94	91.2	97.4	94.3
LR[46]	94.62	-	94.62	-
VAE	99.79	98.57	98.55	98.56

The finding indicates that the suggested VAE model is capable of identifying and categorizing a cloud-based cyber threat with good and consistent performance metrics. The learning curves and confusion matrix are used to corroborate the stability of the convergence and low misclassification. The VAE has a higher overall reliability and solidness in monitoring cloud cybersecurity, in comparison with other ML and DL models.

5. Conclusion and Future Study

Cloud Computing offers a fresh platform on which applications can be developed, and infrastructure can be administered and a dynamic thread space is created with its distributed and elastic character. Modern and dynamic environments of agility and cloud-natives do not support classic security methods to combat cyber-threats. To sum up, the proposed Variational Autoencoder (VAE) model has proven to be very efficient in identifying and categorizing Distributed Denial of Service (DDoS) attacks in cloud systems. The model was remarkably accurate with a precision of 99.79 with balanced (98.57) recall (98.55) and F1-score (98.56) which illustrates the good and consistent results of the model against all the important evaluation measures. The outcome is the capability of the VAE to distinguish correctly the normal and malicious traffic, reducing the rates of false positives and false negatives. The VAE is continually more effective than the traditional machine learning and deep learning models, which means that the former is more capable to process complex and high-dimensional data. This shows that the model is not only dependable but also very strong hence can make it a useful and effective solution to intelligent cloud cybersecurity monitoring. Together, the research proves that the VAE has a

great prospect to better the security of the cloud systems through the ability to identify cyber threats in a timely, accurate and effective manner.

To continue the research in the future, the paper can examine how the VAE model could be used alongside real-time cloud traffic monitoring systems, to further adapt it to new DDoS attack trends, and to train it alongside other deep learning frameworks in a hybrid manner. Also, it can be further enhanced with more experiments and adversarial situations, which would enhance robustness and extrapolation.

References

[1] G. Modalavalasa and S. Pillai, "Exploring Azure Security Center : A Review of Challenges and Opportunities in Cloud Security," *ESP J. Eng. Technol. Adv.*, vol. 2, no. 2, pp. 176–182, 2022, doi: 10.56472/25832646/JETA-V2I2P120.

[2] G. Maddali, "An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 03, May 2025, doi: 10.14741/ijcet/v.15.3.4.

[3] V. Shah, "Traffic Intelligence in IoT and Cloud Networks: Tools for Monitoring, Security, and Optimization," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 5, 2024.

[4] A. Meshram, "Hybrid Cloud Strategy For Mission Critical Financial Software Applications," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 14, no. 12, 2025.

[5] G. M. Sam Prakash Bheri, "Advancements in cloud computing for scalable web development: Security challenges and performance optimization," *J. Comput. Technol. Int. J*, vol. 13, no. 12, 2024.

[6] G. Modalavalasa, "Analysis and Optimization of Privacy-Preserving Encryption Techniques in Cloud Computing Environments for Secure Cloud Data," in *2025 5th International Conference on Intelligent Technologies (CONIT)*, IEEE, Jun. 2025, pp. 1–6. doi: 10.1109/CONIT65521.2025.11167685.

[7] G. Modalavalasa, "Zero-Trust Data Architecture For Multi-Cloud Environments: A Governance-Centric Engineering Approach," *Acta Sci.*, vol. 26, no. 2, pp. 714–726, 2025.

[8] G. Modalavalasa and P. Yadav, "A Hybrid Approach to Cloud Database Security: Integrating DL and Machine Learning for Threat Detection and Prevention," in *2025 3rd International Conference on Inventive Computing and Informatics (ICICI)*, IEEE, Jun. 2025, pp. 1147–1154. doi: 10.1109/ICICI65870.2025.11069530.

[9] F. C. Ogenyi, C. N. Ugwu, and O. P.-C. Ugwu, "Securing the future: AI-driven cybersecurity in the age of autonomous IoT," *Front. Internet Things*, 2025, doi: 10.3389/friot.2025.1658273.

[10] Vaidehi Shah, "Managing Security and Privacy in Cloud Frameworks: A Risk with Compliance Perspective for Enterprises," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 1–13, 2022.

[11] V. Verma, "Big Data and Cloud Databases Revolutionizing Business Intelligence," *Tijer – Int. Res. J.*, vol. 9, no. 1, pp. 48–58, 2022.

[12] V. Shah, "Securing the Cloud of Things: A Comprehensive Analytics of Architecture, Use Cases, and Privacy Risks," *J. Glob. Res. Electron. Commun.*, vol. 3, no. 4, pp. 158–165, 2023, doi: 10.56472/25832646/JETA-V3I8P118.

[13] Anirudh Parupalli and Honie Kali, "An In-Depth Review of Cost Optimization Tactics in Multi-Cloud Frameworks," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 1043–1052, Jun. 2023, doi: 10.48175/IJARSCT-11937Q.

[14] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry (Basel).*, 2017, doi: 10.3390/sym9080164.

[15] M. Gupta, M. Kumar, and R. Dhir, "Unleashing the prospective of blockchain-federated learning fusion for IoT security: A comprehensive review," 2024. doi: 10.1016/j.cosrev.2024.100685.

[16] A. Nawaz, W. Iqbal, A. Altaf, A. Almjally, H. AlSagri, and B. Alabdullah, "CATcAFSMs: Context-based adaptive trust calculation for attack detection in fog computing based smart medical systems," *Expert Syst.*, 2025, doi: 10.1111/exsy.13687.

[17] G. Modalavalasa, "Strengthening Threat Detection and Mitigation Strategies in Cybersecurity with Artificial Intelligence," in *2025 5th International Conference on Intelligent Technologies (CONIT)*, IEEE, Jun. 2025, pp. 1–6. doi: 10.1109/CONIT65521.2025.11166691.

[18] V. Shah, "Analyzing Traffic Behavior in IoT-Cloud Systems : A Review of Analytical Frameworks," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 9, no. 3, pp. 877–885, 2023.

[19] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *J. Netw. Comput. Appl.*, 2016, doi: 10.1016/j.jnca.2016.09.002.

[20] L. Nanjie, "Internet of Vehicles: Your next connection," *Huawei WinWin*, 2011.

[21] S. Narang and V. Gopi Kolla, "Next-Generation Cloud Security: A Review of the Constraints and Strategies in Serverless Computing," *Int. J. Res. Anal. Rev.*, vol. 12, no. 3, 2025, doi: 10.56975/ijrar.v12i3.319048.

[22] S. A. Satyadhar Kumar Chintagunta, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 756–768, 2022.

[23] N. Perlroth, "Security Researchers Find a Way to Hack Cars," The New York Times.

[24] K. Liu, X. Xu, M. Chen, B. Liu, L. Wu, and V. C. S. Lee, "A Hierarchical architecture for the future internet of vehicles," *IEEE Commun. Mag.*, 2019, doi: 10.1109/MCOM.2019.1800772.

[25] A. Syed, *AI-Powered Threat Detection and Mitigation*. Supply Chain Software Security: AI, IoT, and Application Security, 2024. [Online]. Available:

[26] https://scholar.google.com/citations?view_op=view_citation&hl=en&user=T570weEAAAAJ&citation_for_view=T570weEAAAAJ:Y0pCki6q_DkC

[27] S. Singamsetty, "HEALTHCARE IOT SECURITY: EXAMINING SECURITY CHALLENGES AND

SOLUTIONS IN THE INTERNET OF MEDICAL THINGS. A BIBLIOMETRIC PERSPECTIVE," *J. Popul. Ther. Clin. Pharmacol.*, 2024, doi: 10.53555/7j8dhs24.

[28] M. Lombardi, F. Pascale, and D. Santaniello, "Two-Step Algorithm to Detect Cyber-Attack Over the Can-Bus: A Preliminary Case Study in Connected Vehicles," *ASCE-ASME J. Risk Uncertain. Eng. Syst. Part B Mech. Eng.*, 2022, doi: 10.1115/1.4052823.

[29] A. Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial internet of things," *Digit. Commun. Networks*, 2023, doi: 10.1016/j.dcan.2022.09.008.

[30] A. N. Jahromi, H. Karimipour, and A. Dehghantanha, "An ensemble deep federated learning cyber-threat hunting model for Industrial Internet of Things," *Comput. Commun.*, 2023, doi: 10.1016/j.comcom.2022.11.009.

[31] M. Al-Omari, M. Rawashdeh, F. Qutaishat, M. Alshira'H, and N. Ababneh, "An Intelligent Tree-Based Intrusion Detection Model for Cyber Security," *J. Netw. Syst. Manag.*, 2021, doi: 10.1007/s10922-021-09591-y.

[32] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," *Symmetry (Basel).*, 2020, doi: 10.3390/SYM12050754.

[33] F. Alserhani, "Analysis of Encrypted Network Traffic for Enhancing Cyber-security in Dynamic Environments," *Appl. Artif. Intell.*, 2024, doi: 10.1080/08839514.2024.2381882.

[34] N. Imtiaz *et al.*, "A Deep Learning-Based Approach for the Detection of Various Internet of Things Intrusion Attacks Through Optical Networks," *Photonics*, 2025, doi: 10.3390/photonics12010035.

[35] T. Yesuraju, S. M. Vali, S. Sameer, S. Shabbir, and S. Riyaz, "Enhancing Network Security: A Comparative Analysis of Machine Learning, Ensemble Methods, and Federated Learning for Intrusion Detection," 2025. doi: 10.1109/icoici65217.2025.11254279.

[36] N. Venkatesh, V. K. Pidatala, S. M. Hemalatha, P. Matam, R. Stalinbabu, and S. S, "AI-Driven Threat Intelligence Framework for Real-Time Cybersecurity using Federated Deep Learning and Cloud Orchestration," 2025. doi: 10.1109/icoici65217.2025.11254858.

[37] E. V. N. Jyothi, M. Kranthi, S. Sailaja, U. Sesadri, S. N. Koka, and P. C. S. Reddy, "An Adaptive Intrusion Detection System in Industrial Internet of Things(IIoT) using Deep Learning," in *Proceedings - 2024 1st International Conference on Innovative Sustainable Technologies for Energy, Mechatronics and Smart Systems, ISTEMS 2024*, 2024. doi: 10.1109/ISTEMS60181.2024.10560245.

[38] D. Tocci, R. Zhou, and K. Zhang, "FPGA Accelerated Decentralized Reinforcement Learning for Anomaly Detection in UAV Networks," in *2023 IEEE 16th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC)*, 2023, pp. 248–253. doi: 10.1109/MCSoC60832.2023.00044.

[39] S. Divakar, R. Priyadarshini, R. K. Barik, and D. S. Roy, "An intelligent intrusion detection scheme powered by boosting algorithm," in *Proceedings of the Confluence 2021: 11th International Conference on Cloud Computing, Data Science and Engineering*, 2021. doi: 10.1109/Confluence51648.2021.9377076.

[40] V. Patel, S. Choe, and T. Halabi, "Predicting Future Malware Attacks on Cloud Systems using Machine Learning," in *Proceedings - 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, IDS 2020*, 2020. doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00036.

[41] M. M. Saad, T. Iqbal, H. Ali, M. F. Bulbul, S. Khan, and C. Tanougast, "Incident Detection over Unified Threat Management Platform on a Cloud Network," in *Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*, 2019. doi: 10.1109/IDAACS.2019.8924299.

[42] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," *2nd Int. Conf. Learn. Represent. ICLR 2014 - Conf. Track Proc.*, no. Ml, pp. 1–14, 2014, doi: 10.61603/ceas.v2i1.33.

[43] N. S. M. V. Sri Hari Deep Kolagani, "Human-in-the-Loop and Generative AI Dilemma: A Hybrid Strategy for Effective Customer Service in Enterprise CRM," *Int. J. Bus. Technol. Manag.*, vol. 7, no. 10, pp. 233–239, Dec. 2025, doi: 10.55057/ijbtm.2025.7.10.18.

[44] S. Azmin and A. B. M. A. Al Islam, "Network Intrusion Detection System based on Conditional Variational Laplace AutoEncoder," in *7th International Conference on Networking, Systems and Security*, New York, NY, USA: ACM, Dec. 2020, pp. 82–88. doi: 10.1145/3428363.3428371.

[45] V. Jyothsna, A. C. Manisha, B. NanduSri, K. Poorna Chandhu, A. Leela Rama Seshu, and G. Mahalakshmi Manasvi, "Intrusion Detection System for Detection of DDoS Attacks in Cloud Environment," *Res. Sq.*, 2023.

[46] G. Prabhakar and B. B. Rao, "Enhanced Deep Learning-Based Security Model for Data in Cloud," *SSRG Int. J. Electron. Commun. Eng.*, 2025, doi: 10.14445/23488549/IJECE-V12I3P108.

[47] M. Bakro *et al.*, "Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along With Random Forest Model," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3353055.