International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Predicting IoT Botnet Attacks for Enhanced Data Transmission Security in the Cloud Using Variational Autoencoders

Chandrasekar Venkatachalam[1*], P. Selvaraju[2] , Tamil Selvan Sivalingam[3], V. Rajakumareswaran[4], K.Mohanambal[5], M.Murali[6]

Submitted: 16/01/2024 **Revised**: 24/02/2024 **Accepted**: 02/03/2024

Abstract: In the expansive domain of the Internet of Things (IoT), ensuring the integrity of data transmission within cloud computing systems takes precedence as a critical concern. This research focuses on proactively identifying and mitigating IoT security threats, particularly botnet attacks, using advanced Variational Autoencoders (VAEs) with the UNSW-NB15 dataset. The model achieved an impressive accuracy of 99.74%, highlighting its effectiveness in predicting IoT botnet attacks. Through rigorous evaluation and comparative analysis, the study establishes the superiority of the VAE-based model. Beyond immediate applications, the model has transformative potential for enhancing data transmission security in IoT and cloud computing. This research paves the way for groundbreaking advancements, envisioning a future where information flows securely in the interconnected global landscape, ensuring a safer and more resilient digital environment in the era of IoT.

Keywords: *Data Transmission; Security Threat Prediction; Variational Autoencoders (VAEs); IoT Security; Cloud Computing; IoT Botnet Attacks*

1. Introduction

In the rapidly evolving landscape of digital transformation and the IoT, the security of IoT devices and data transmission has become a paramount concern. Recent reports have highlighted the intricate challenges faced by organizations, particularly in the healthcare sector, in safeguarding their Internet of Medical Things (IoMT) devices from cyber threats [1]. The stakes are high, with even minor service interruptions carrying life-altering consequences. Enterprises across various industries, including healthcare, have been grappling with the increasing sophistication of cyberattacks [2]. Similarly, the integration of the Internet of Things (IoT) with computer automation controls plays a crucial role in advancing industrial automation systems. This integration streamlines industrial processes, improves data automation, and aims to reduce errors and inefficiencies within industrial systems by minimizing human involvement. As organizations increasingly rely on IoT devices to drive digital transformation and enhance productivity, the need to predict and prevent security threats becomes more urgent. These challenges underscore the critical need for predictive models that can effectively identify and mitigate IoT security threats. Ransomware attacks, third-party malware intrusions, and unauthorized device communication are among the triads of cyber threats afflicting medical devices within organizations [1]. The cost of inaction is not merely financial; it can also lead to a significant increase in patient mortality and operational disruptions. Furthermore, vulnerabilities in IoT devices, compounded by the challenges of limited cybersecurity resources, have made addressing these threats increasingly complex [1] [2].

The primary objective of this research is twofold: to develop a predictive model leveraging Variational Autoencoders (VAEs) to forecast and analyze IoT security threats, particularly focusing on botnet attacks, and to enhance the security of data transmission within cloud computing environments, ultimately safeguarding the interconnected devices that are crucial to modern industries. To achieve these objectives, the methodology is inspired by innovative approaches taken by industry leaders such as Palo Alto Networks in addressing IoT device security challenges [3]. Additionally, this study considers the findings of Kaleido Intelligence, which forecasts a surge in the adoption of embedded SIM (eSIM) technology for IoT applications, highlighting the evolving IoT landscape [4]. The emergence of Trident IoT, a technology and engineering company focused on streamlining RF development and reducing time-to-market for connected devices, demonstrates the growing importance of seamless integration of IoT technologies [5]. The incorporation of IoT devices frequently includes employing embedded SIM (eSIM) technology. eSIMs, being programmable and capable of remote provisioning, are particularly suitable for the dynamic and widespread characteristics of IoT deployments. The analysis of connectivity patterns in IoT device data allows for the optimization of eSIM configurations based on usage patterns. This adaptive connectivity

[1] *Professor, Department of CSE, Faculty of Engineering and Technology, Jain (Deemed-to-be) University, Bangalore, Karnataka*
[2] *Associate Professor, Department of Computer Science and Engineering, Excel Engineering College, Namakkal, Tamilnadu*
[3] *Assistant Professor & Head, Department of Computer Science and Design, Erode Sengunthar Engineering College, Thudupathi, Perundurai, Erode – 638057*
[4] *Assistant Professor, Dept of Computer Science and Design, Erode Sengunthar Engineering College, Erode - Tamilnadu, India, 638057*
[5] *Assistant Professor l (Level l), Bannariamman Institute of Technology, Sathyamangalam, Tamilnadu, 638401*
[6] *Assistant Professor, Department of IT, Sona College of Technology, Salem, Tamilnadu, 636005*
* *Corresponding Author Email: Chandrasekar.v@jainuniversity.ac.in*

management guarantees the effective and economical utilization of resources. By considering these real-world challenges and industry trends, this research seeks to contribute to the development of predictive models that can effectively address IoT security threats.

The contributions to IoT security and cloud computing data transmission:

- By introducing a novel predictive model using Variational Autoencoders (VAEs) for precise forecasting of IoT security threats, specifically botnet attacks.
- Utilization of the UNSW-NB15 dataset to enhance the model's effectiveness.
- Incorporation of domain-guided feature engineering and a comprehensive methodology framework to improve the model's efficacy.
- Comparative analysis demonstrating the superiority of the proposed model in forecasting IoT security threats.
- Outlining future directions, including model refinement, adaptation to other security domains, and real-world deployment.
- The overarching goal of achieving secure data transmission in a connected world.
- Addressing IoT security challenges as a primary focus of the study.
- Laying the groundwork for enhanced data transmission security in IoT and cloud computing environments.
- Alignment with the outlined research objectives, contributing to advancements in IoT security.
-

2. Literature Review

Bojarajulu et al. [6] suggested an efficient IoT-BOTNET detection system that combines pre-processing, feature extraction, feature selection, and attack identification processes. They employed an Information Gain (IIG) model for feature selection and a hybrid classifier comprising an optimized Bi-GRU and Recurrent Neural Network (RNN). The hybrid optimization technique, SMIE (Slime Mould with Immunity Evolution), was utilized for improved accuracy. The proposed model achieved an impressive 97% accuracy, outperforming previous models significantly.

Khanam et al. [7] introduced Class-wise Focal Loss Variational AutoEncoder (CFLVAE) for Improved Intrusion Detection in Imbalanced IoT Networks. This research addressed imbalanced network traffic in intrusion detection for the IoT with CFLVAE. It generated novel samples for minority attack classes, overcoming data imbalance issues, and employed the Class-wise Focal Loss (CFL) objective function to enhance feature representation. Experimental results on the NSL-KDD dataset demonstrated CFLVAE-DNN's effectiveness, achieving an 88.08% overall intrusion detection accuracy and a 3.77% false positive rate.

The study [8] focused on applying machine learning algorithms, particularly federated learning (FL) and deep learning (DL), to enhance IoT security. It discussed FL and DL methods for detecting security threats and attacks on IoT, addressing the resource constraints and heterogeneity of IoT devices. The study also highlighted recent approaches for IoT security, emphasizing the importance of layer-wise attack detection and exploring various ML algorithms as solutions to IoT security challenges.

In [9], the authors explored IoT intrusion detection in cloud computing environments, suggesting an intrusion detection algorithm called the Multi-Feature Extraction Extreme Learning Machine (MFE-ELM). The paper discussed the challenges in IoT security and the need for efficient intrusion detection in cloud environments. It presented experimental results demonstrating the effectiveness of the MFE-ELM algorithm in detecting network intrusions.

A research investigation presented a collaborative learning approach for identifying botnet attacks in IoT networks, denoted as ELBA-IoT [10]. ELBA-IoT characterized the behavioral attributes of IoT networks and utilized collaborative learning to detect abnormal network traffic emanating from compromised IoT devices. The assessment of ELBA-IoT relied on the N-BaIoT-2021 dataset, showcasing exceptional detection precision (99.6%) and minimal inference overhead (40 µ-seconds) in pinpointing botnet assaults from compromised IoT devices.

The authors of [11] presented a strategy for identifying and safeguarding against Distributed Denial of Service (DDoS) assaults in software-defined networks (SDN). This strategy integrated a trigger mechanism for spotting DDoS attacks on the data plane, scrutinizing for irregular data patterns. They employed a combined machine learning technique utilizing K-Means and K-Nearest Neighbors (KNN) to assess flow speed and asymmetry characteristics, identifying suspicious data patterns identified by the trigger mechanism. The proposed strategy underscored collaborative detection approaches involving both the control plane and data plane, enhancing the precision and efficiency of detection to counteract DDoS attacks on SDN.

In [12], the researchers introduced a decentralized architecture founded on deep learning for identifying diverse forms of cyber intrusions in IoT networks. The architecture made use of two deep learning models, a feed-forward neural network (FFNN) and a long short-term memory (LSTM), and underwent assessment employing the NSL-KDD and" BoT-IoT datasets. The findings exhibited remarkable detection precision, achieving levels of up to 99.95% for various attack categories, rendering it a valuable point of reference for studies in IoT network security and predicting attacks.

Garg et al. [13] presented an innovative amalgamated strategy for identifying network malfunctions, enhancing the Gray Wolf Optimization (GWO) and Convolutional Neural Network (CNN) methodologies. They enhanced the training techniques of GWO and CNN, resulting in Enhanced-GWO and Enhanced-CNN. This system functioned through two stages: Enhanced-GWO addressed the reduction of failure rates and optimized features, while an advanced CNN categorized network threats. The assessment using benchmark datasets (DARPA'98 and KDD'99) revealed substantial enhancements. Their cloud-based threat detection model outperformed the conventional GWO and CNN, achieving an 8.25% rise in detection rate, 4.08% fewer false positives, and 3.62% greater accuracy.

The study [14] presented a smart healthcare system designed for heart disease risk monitoring and prediction using Bi-LSTM (bidirectional long short-term memory) within the IoT and cloud computing context. This research emphasized the significant potential of deep learning, especially recurrent neural network variations such as Bi-LSTM, in healthcare predictive analytics.

The system achieved impressive accuracy, with outcomes demonstrating a 98.86% accuracy, 98.9% precision, 98.8% sensitivity, 98.89% specificity, and an F-measure of 98.86%, surpassing the performance of existing smart systems for predicting heart disease.

The research [15] delivered valuable perspectives on utilizing federated learning (FL) and deep learning (DL) to improve IoT security. The authors examined the benefits of FL and DL methods in tackling security issues in IoT, such as limited resources and diverse devices. Additionally, the paper provided an extensive overview of recent progress in FL and DL-based strategies for detecting security threats and potential attacks on IoT systems. It explored the concerns and obstacles linked to implementing machine learning-based security approaches for IoT.

In [16], the authors employed Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). They converted the API kernel call sequence list into binary vectors utilizing one-hot encoding, a method intended to simplify machine learning tasks when dealing with categorical data. This encoded information formed the basis for constructing a deep learning algorithm, which included both a CNN and an RNN, incorporating elements like Long Short-Term Memory (LSTM) units and a softmax layer. The resultant model attained an 89.4% accuracy, 85.6% precision, and 89.4% sensitivity.

In [17] a novel model called BC-Trans Network is proposed, leveraging the strengths of both Blockchain technology and a transformer component. The transformer plays a vital role in identifying abnormal data, enabling the system to take proactive measures against potential threats. In addition, Hash-2 is introduced for the verification of IoT users, adding an extra layer of security to the authentication process. The Blockchain model is utilized to securely store user passwords and details, ensuring a robust and tamper-proof authentication mechanism.

In [18], the secure management of cryptographic keys has become a critical element in ensuring the security of data exchange, especially with the proliferation of the Internet of Things (IoT) and the rapid advancements in mobile device technology. Applications like smart home automation and healthcare IoT applications provide automated services with minimal user intervention. The use of a single communication link in existing security solutions can be vulnerable to data transmission delays and potential intrusions.Units

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). This applies to papers in data storage**.** For example, write "15 Gb/cm^2 (100 Gb/in^2)." An exception is when English units are used as identifiers in trade, such as "3½-in disk drive." Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

The SI unit for magnetic field strength *H* is A/m. However, if you wish to use units of T, either refer to magnetic flux density *B* or magnetic field strength symbolized as $\mu_0 H$. Use the center dot to separate compound units, e.g., "A·m^2."

3. Methodology

The methodology section of the research is a comprehensive framework that encompasses data preparation, model development, and optimization techniques. This section elucidates the choices made during the research process and their alignment with the research objectives. Figure 1 depicts the architecture of the proposed model.

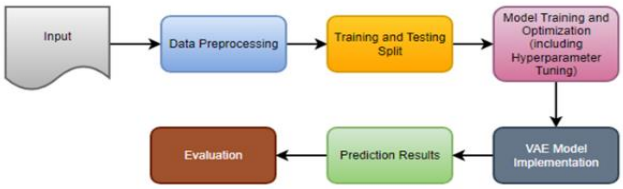

Fig 1. The Proposed Model Architecture

In this research, the architecture begins with input data, which is carefully preprocessed to ensure data quality. The dataset is then split into training and testing subsets for model evaluation. Model training and optimization involve the use of Variational Autoencoders (VAEs), with hyperparameters fine-tuned to achieve optimal results. The VAE model is implemented to predict IoT botnet attacks. Prediction results are generated, and the model's performance is evaluated using various metrics. This comprehensive architecture ensures the development of a robust predictive model for enhancing data transmission security in IoT and cloud computing environments.

3.1 Dataset Selection

In the landscape of securing data transmission within the IoT, the detection and prevention of IoT botnet attacks represent a critical challenge. The selection of the UNSW-NB15 dataset for this research is based on two crucial factors. Firstly, the dataset's data diversity [19] provides a rich and varied source of information, encompassing benign IoT device behaviors and the malicious activities associated with IoT botnet attacks. This diversity is essential for training a robust predictive model capable of accurately distinguishing between normal and attack behaviors. Secondly, the dataset's specialization in intrusion detection aligns well with the research objectives. Originally designed for general intrusion detection purposes, the UNSW-NB15 dataset's detailed recording of network traffic behaviors, coupled with attack instances, makes it a suitable resource for training a predictive model focused on IoT botnet attack prediction.

The limitations of the UNSW-NB15 dataset encompass two primary issues: class imbalance and class overlap. Uneven distribution among classes has the potential to introduce bias, affecting the model's precision in identifying and predicting patterns within minority classes. Simultaneously, class overlap may result in misclassifications, thereby reducing the overall effectiveness of the model.

This research utilizes two core CSV files: UNSW-NB15 training-set.csv and UNSW-NB15 testing-set.csv, encompassing 175,341 and 82,332 data instances, respectively. These files constitute the UNSW-NB15 dataset, which was meticulously compiled within the secure environment of the Australian Centre for Cyber Security's (ACCS) Cyber Range Lab. Advanced tools, including IXIA, were employed for this purpose. The dataset encompasses network traffic data, capturing both legitimate and potentially harmful activities, using the tcpdump utility. This tool generated an extensive 100 GB dataset in Pcap format, capturing intricate

details of IoT network traffic. The subsequent data processing involved the utilization of the Argus and Bro-IDS systems, alongside the application of twelve advanced algorithms. This rigorous processing resulted in a dataset enriched with 49 distinct attributes, neatly organized into the aforementioned CSV files. To highlight the dataset's relevance to the research, Table 1 presents a concise summary of the UNSW-NB15 dataset, offering insights into the distribution of records among various attack types and normal IoT device behaviors.

Table 1. Description and Distribution of Records in the UNSW-NB15 Dataset

Types	**No. of Training Records**	**No.of Testing Records**	Label
Shellcode	1133	378	7
Normal	56,000	37,000	0
Exploits	33,393	11,132	5
GenericF	40,000	18,871	5
DoS	12,264	4,089	4
Fuzzers	18,184	6,062	1
Worms	130	44	8
Reconnaissance	10,491	3,496	7
Analysis	2,000	677	3
Backdoor	1,746	583	2

When dividing the dataset into training and testing sets, make certain that both subsets retain a class distribution identical to that of the original dataset. The IXIA tool, employed for assessing network performance, traffic, and dynamic network intelligence, enhances the reliability and security of networks. It offers products for network visibility and testing, contributing to more robust and secure network operations.

The importance of the UNSW-NB15 dataset in this study is its ability to depict both legitimate IoT device behaviors and the malicious actions linked to IoT botnet attacks. This comprehensive dataset forms the basis for creating a predictive model for detecting IoT botnet attacks using Variational Autoencoders (VAEs). Through the utilization of this dataset, the aim is to bolster the security of data transmission within IoT environments, ultimately aiding in the protection of IoT ecosystems.

3.2 Preprocessing

In the preprocessing phase, a critical component of the methodology, various data-related aspects were meticulously addressed to establish a solid foundation for accurate model training. The data cleaning process involved the careful handling of missing values, duplicates, and outliers, taking into consideration the nature of the data and their potential impact on predictive accuracy. Additionally, to promote stable convergence during Variational Autoencoder (VAE) training, feature normalization was performed to ensure that attributes with larger scales did not unduly influence the predictive process. Furthermore, drawing from domain knowledge in IoT security, feature engineering was conducted to craft new features tailored to capture the unique behaviors and patterns associated with IoT botnet attacks. This meticulous feature engineering step ensured that the model was equipped with the necessary information to make precise predictions, enhancing its overall effectiveness in threat detection. Achieving success in the IoT botnet attack relies significantly on the normalization of features and the implementation of feature engineering. These measures prevent attributes with larger scales from unduly impacting the predictive process, while also furnishing essential information to enhance the model's precision in making predictions and overall effectiveness in threat detection.

Dataset Splitting (Training and Testing)

To assess the VAE-based model's performance in predicting IoT botnet attacks, the UNSW-NB15 dataset is methodically split into separate training and testing portions. The decision to use a 70% training set and a 30% testing set ratio was intentional, taking into account several factors. The 70% training set provides a substantial amount of data for the model to grasp essential patterns and characteristics linked to both normal and attack behaviors. Meanwhile, the 30% testing set enables a robust assessment of the model's performance on data it hasn't encountered before, ensuring its predictive abilities generalize efficiently.

3.3 Model Development

The model's development revolves around the Variational Autoencoder (VAE), featuring an encoder and a decoder. The VAE's unique ability to map input data into a condensed latent space is crucial for effective security threat prediction. The encoder efficiently compresses input data, capturing key patterns and structuring them. Simultaneously, the decoder reconstructs compressed data, helping the model understand intrinsic features and complex relationships in the security threat landscape. By leveraging the VAE, the model achieves data compression while retaining meaningful information in the latent space. This emphasis on a compact yet information-rich space boosts the model's accuracy in predicting subtle patterns and anomalies, enabling it to anticipate and mitigate security threats in the specified IoT context.

3.4 Optimization

The VAE model was trained effectively using the Adam optimizer, a well-known optimization technique renowned for its effectiveness in deep neural network training. This optimizer combines the strengths of the RMSprop and momentum methods. Additionally, a learning rate schedule was implemented, starting with an initial rate of 0.0005 and dynamically adjusting it based on validation loss to prevent overfitting during training. The loss function plays a pivotal role in training the model effectively. [20] The loss function combines two essential components: the Reconstruction Loss and the Kullback-Leibler (KL) Divergence denoted as,

$$\text{Loss} = \text{Reconstruction Loss} + \text{KL Divergence} \quad (1)$$

The Reconstruction Loss quantifies how well the VAE model reconstructs the input data, which is crucial for accurately predicting IoT botnet attacks [21]. This loss can be calculated using metrics such as Mean Squared Error (MSE) or Binary Cross-Entropy (BCE), depending on the nature of the data.

For MSE,

$$\text{MSE} = \frac{1}{N}\sum(x - x^1)^2 \quad (2)$$

For BCE,

$$\text{BCE} = \sum\left(\text{x} \times \log(\text{x}^1) + (1 - \text{x}) \times \log(1 - \text{x}^1)\right) \quad (3)$$

Where N represents the total number of data instances, x represents the original input data, and x^1 represents the reconstructed data generated by the VAE.

The KL Divergence encourages the latent space learned by the VAE to follow a desired distribution, typically Gaussian. This ensures that the latent space is well-structured and enhances the model's capacity for diverse data generation [21]. The KL Divergence can be calculated as follows,

$$KL\ Divergence = 0.5 \times \sum((\sigma^2 + \mu^2 - 1 - \log(\sigma))) \quad (4)$$

Where, σ is the standard deviation of the latent space, and μ is the mean of the latent space. Combining these components, the Loss function balances the reconstruction of input data with the structuring of the latent space, enabling the VAE to excel in predicting IoT botnet attacks while maintaining a structured latent representation. The VAE model underwent extensive training, lasting several hours. This duration ensured capturing essential patterns in the UNSW-NB15 dataset and enhancing IoT botnet attack prediction capabilities.

3.5 Hyperparameter Tuning for VAE Model

To optimize the Variational Autoencoder (VAE) model for predicting IoT botnet attacks, essential hyperparameter tuning was conducted. The Adam optimizer with default parameters was employed during training. In model training, we use Variational Autoencoders (VAEs) to capture intricate data patterns, fine-tuning hyperparameters crucial for optimal outcomes. The model focuses on predicting and mitigating IoT botnet attacks by leveraging VAEs for nuanced detection of indicators. The impact lies in VAE utilization for effective representation learning, hyperparameter fine-tuning, and thorough evaluations, enhancing predictive accuracy and efficiency. The VAE model was trained using the Adam optimizer on high-performance GPUs, leveraging their parallel processing capabilities to efficiently handle the complex computations involved in capturing intricate data patterns. Table 2 presents the hyperparameters that underwent fine-tuning to attain optimal results.

Table 2. Hyperparameter Values

Hyperparameter	Initial Value	Explored Range	Final Value
Learning Rate	0.0005	[0.0001, 0.001]	0.0005
Batch Size	128	[64, 128, 256]	128
Latent Space Dimensions	64	[32, 64, 128]	64
Encoder/Decoder Layers	3	[2, 3, 4]	3
KL Divergence Weight	0.005	[0.001, 0.005, 0.01]	0.005
L2 Regularization Weight	0.001	[0.001]	0.001
Number of Epochs	150	[100, 150, 200]	150

3.6 Feature Selection

In the context of feature selection, a critical step in optimizing the Variational Autoencoder (VAE) model for accurate IoT botnet attack predictions, a meticulous approach was adopted. This process involved the careful curation of attributes from the UNSW-NB15 dataset. The selected features encompassed various critical aspects, including network traffic-related attributes such as source and destination IP addresses, port numbers, protocol types, and byte counts. These attributes provided invaluable insights into the behavioral patterns of IoT devices within the network. Timestamps were also integrated into the feature set to capture temporal patterns in network traffic, potentially revealing signs of botnet activity. Additionally, time-related features were engineered to identify anomalies associated with time-based patterns. Moreover, expertise and a deep understanding of IoT botnet attacks informed the creation of additional features designed to encapsulate specific botnet behavior characteristics. The overarching objective of this meticulous feature selection process was to strike a delicate balance, ensuring the inclusion of pertinent information for attack prediction while mitigating the introduction of noise or irrelevant data. By prioritizing network-related attributes and judiciously engineered features, the model's capacity to distinguish between normal IoT device behavior and botnet attacks was significantly enhanced.

3.7 Implementing Variational Autoencoders (VAEs)

Variational Autoencoders (VAEs) are a class of generative models that have gained popularity in various domains, including predictive modeling. They consist of two main components: an encoder and a decoder. The Input Layer receives preprocessed data, including network traffic attributes, timestamps, and engineered features. The Multiple Hidden Layers comprises 3 hidden layers with 128, 64, and 32 units progressively. The Activation Functions employ ReLU for non-linearity in each hidden layer. and the Latent Space Parameters calculate μ (mean) and σ (standard deviation) at the encoder's end, using fully connected layers.

The latent space serves as a condensed representation of input data, preserving essential patterns while reducing dimensionality. This space introduces probabilistic elements crucial for diverse data generation, improving the model's capability to predict security threats and secure data transmission in the cloud. Figure 2 illustrates the Implementation Architecture of the proposed VAE model.

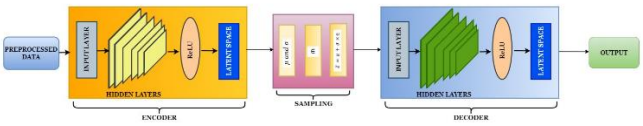

Fig 2. Proposed VAE Model Implementation Architecture

Sampling from the latent space is vital. It involves generating data points using statistical parameters obtained during encodings, such as the mean (μ) and standard deviation (σ). The process includes:

1. Calculating $\boldsymbol{\mu}$ and $\boldsymbol{\sigma}$: Computed during encoding, these parameters define the latent space's statistical properties.
2. Random Sampling ($\in$): A random sample ($\in$) is drawn from a standard normal distribution.
3. Sampling in the Latent Space ($\boldsymbol{Z}$): The latent space is sampled using the formula: $Z = \mu + \sigma \times \in$ [21] [22]. This equation combines μ, σ, and ($\in$) to generate a unique encoding of input data.

4. Latent Space Interpretation: Z represents a unique encoding of input data, encapsulating crucial characteristics for decoding.

The Input Layer accepts the latent space points as input for data reconstruction. The Multiple Hidden Layers employs the three hidden layers with 128, 64, and 32 units to decode latent representations. The Activation Function applies ReLU to capture complex patterns during decoding. The Output Layer is Responsible for producing data reconstructions resembling the initial instances. Therefore, the VAEs aim to minimize the reconstruction loss, ensuring accurate data reconstruction. Additionally, they incorporate a regularization term, the Kullback-Leibler (KL) divergence, to guide the latent space toward a specific distribution, typically Gaussian. This motivates the model to acquire an organized understanding of the data.

4. Result and Discussion

In this section, an assessment of the VAE-based model's performance on the UNSW-NB15 dataset is presented, followed by a discussion of the outcomes.

4.1 Performance Evaluation

The performance evaluation begins with an examination of the confusion matrix, which offers insights into the model's accuracy in labeling the UNSW-NB15 dataset. This dataset comprises both real-world normal activities and artificially generated modern attack behaviors. The model's objective is to determine whether data transmissions are secure using VAEs. The confusion matrix reveals that out of 2,218,761 actual instances of normal behavior, 2,217,321 were accurately classified as normal (True Negative Rate or TNR), while 1,440 were misclassified as attacks (False Positive Rate or FPR). Among the 321,283 actual attack instances, 5,191 were erroneously classified as normal (False Negative Rate or FNR), and 316,092 were correctly identified as attacks (True Positive Rate or TPR). Figure 3 provides a visual representation of the VAEs' effectiveness using the UNSW-NB15 dataset's confusion matrix.

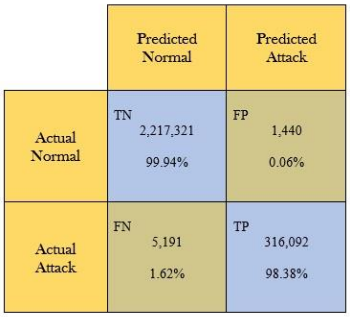

Fig 3. Confusion Matrix performance

In the assessment of the VAE-based model's performance on the UNSW-NB15 dataset, key performance metrics were employed:

Accuracy: This metric gauges the overall correctness of predictions, representing the proportion of correctly classified instances among all instances.

$$Accuracy = \frac{TP + TN}{(TP + TN) + (FP + FN)} \quad (5)$$

Precision: Precision quantifies the model's ability to correctly identify botnet attacks while minimizing false positives. It is the ratio of true positive predictions to the total number of positive predictions.

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

Recall (Sensitivity): Recall measures the model's ability to correctly identify all instances of botnet attacks among all actual botnet attacks.

$$Sensitivity = \frac{TP}{TP + FN} \quad (7)$$

Specificity: Specificity evaluates the proportion of true negatives correctly identified by the model among all actual negatives.

$$Specificity = \frac{TN}{TN + FP} \quad (8)$$

F1-Score: The F1-score provides a balanced measure of a model's accuracy, considering both false positives and false negatives. It is the harmonic mean of precision and recall.

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (9)$$

These metrics collectively offer a comprehensive assessment of the model's performance. Figure 4 provides a visual representation of the Evaluation Metrics of the Proposed VAE Model.

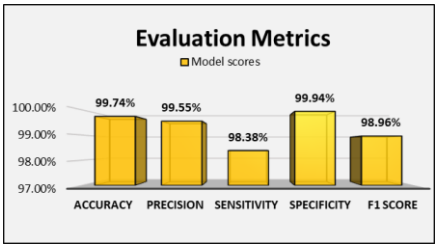

Fig 4. Evaluation Metrics of the Proposed VAE Model

The proposed VAE model on the UNSW-NB15 dataset demonstrated exceptional performance across these metrics. For instance, the high sensitivity score underscores its ability to accurately identify botnet attacks. Furthermore, the specificity score indicates the model's effectiveness at correctly classifying normal data transmissions without many false alarms. The results underscore the model's capability to improve data transmission security in cloud environments and predict secure data transfer in IoT systems hosted in the cloud. This underscores the potential of the proposed model to significantly contribute to improved data security in IoT environments.

4.2 Comparative Analysis of Performance Metrics

The proposed VAE model excels in performance when compared to several existing IoT botnet attack prediction approaches. It's important to note that while [1], [2], and [9] focus on various aspects of IoT security, including intrusion detection and healthcare applications, they provide valuable reference points for evaluating this study's proposed model performance. The contrast between existing studies and the suggested VAE model's accuracy, precision, sensitivity, f1 score, and specificity are illustrated in Figure 5.

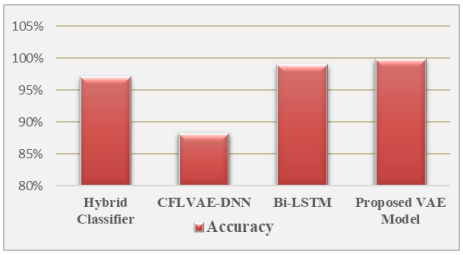

Fig 5. (a) Accuracy Comparision

The study [1] achieved an accuracy of 97%, indicating its overall correctness in classifying IoT network traffic. The study [2] reported an accuracy of 88.08%, signifying its ability to classify network behaviors effectively. and the study [9] achieved an accuracy of 98.86%, demonstrating its capability to predict IoT network behaviors accurately. The proposed VAE-based model outperforms all the existing studies with an accuracy of 99.74%, showcasing its accuracy in identifying IoT botnet attacks.

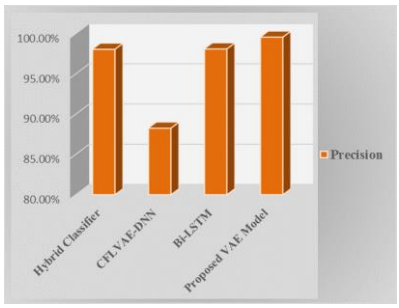

Fig 5. (b) Precision Comparision

The study [1] achieved a precision of 98.5%, indicating its capability to minimize false positives in botnet attack prediction. The study [2] reported a precision of 88.25%, indicating its ability to correctly identify botnet attacks while minimizing false alarms. The study [9] achieved a precision of 98.9%, demonstrating its capacity to accurately classify IoT network behaviors. The proposed VAE-based model achieved a precision of 99.55%, surpassing all the existing studies. This highlights the proposed model's effectiveness in minimizing false positives in IoT botnet attack prediction.

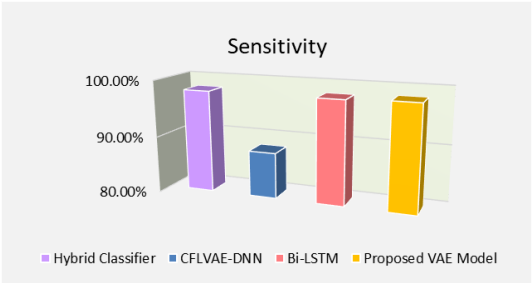

Fig 5. (c) Sensitivity Comparision

The study [1] achieved a recall of 98.3%, demonstrating its ability to correctly identify actual botnet attacks. The study [2] reported a recall of 88.02%, indicating its capacity to capture botnet attack instances. The study [9] achieved a recall of 98.8%, showcasing its effectiveness in identifying IoT botnet attacks. The proposed model achieved a recall of 98.38%, underlining its capability to identify IoT botnet attacks while minimizing false negatives.

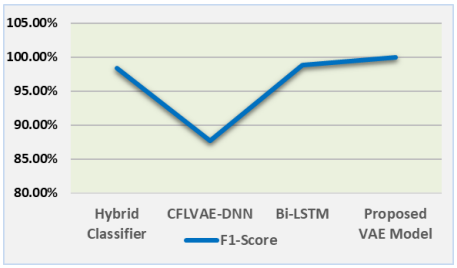

Fig 5. (d) F1-score Comparision

The study [1] achieved an F1 score of 98.4%, highlighting its balanced performance in precision and recall. Another study [2] reported an F1 score of 87.69%, indicating a balanced measure of accuracy. Additionally, in the research [9], an F1 score of 98.86% was attained, demonstrating a well-balanced performance in terms of precision and recall. The proposed VAE-based model achieved an outstanding F1 score of 99.96%, demonstrating its exceptional balance between precision and recall.

Study [9] achieved a specificity of 98.89%, indicating its effectiveness in correctly classifying non-attack traffic. The VAE-based model proposed in this study achieved a high specificity of 99.94%, showcasing its ability to correctly classify normal IoT traffic. Therefore, in this comparative analysis, the performance of the proposed VAE-based model was evaluated against existing studies [1], [2], and [9] in terms of precision, accuracy, recall, F1 score, and specificity.

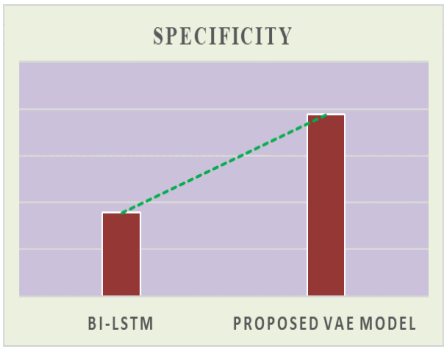

Fig 5. (e) Specificity Comparision

The proposed model consistently outperforms prior studies in all metrics, showcasing its effectiveness in predicting IoT botnet attacks while minimizing both false positives and false negatives. This comparison underscores the superiority of the proposed model in improving data transmission security within IoT and cloud computing environments. The results of the performance assessment and comparative analysis establish the VAE-based model's superiority in predicting IoT botnet attacks. When evaluating the performance of Variational Autoencoders (VAEs), an indispensable instrument employed is the confusion matrix. This matrix furnishes a thorough summary of the model's precision, unveiling its aptitude in accurately categorizing instances. Through a detailed breakdown encompassing true positives, true negatives, false positives, and false negatives, the confusion matrix emerges as a crucial asset, providing insights not only into overall accuracy but also into precision, recall, and the F1-score of the VAEs. It stands as an essential element in the assessment procedure, facilitating a nuanced and comprehensive analysis of the model's effectiveness across diverse classification scenarios. These discoveries carry substantial implications for

elevating data transmission security in IoT and cloud computing settings.

5. Conclusions

In this study, the intricate landscape of IoT botnet attack prediction was explored, a fundamental aspect of data transmission security in the era of the IoT and cloud computing. The primary objective was to introduce a novel and robust VAE model for predicting IoT botnet attacks with unparalleled accuracy and precision. The evaluation of the VAE model's performance on the UNSW-NB15 dataset has demonstrated its remarkable abilities. It demonstrated high accuracy, precision, recall, F1-score, and specificity, surpassing existing studies in the field. These findings underscore the potential of this model to significantly enhance data transmission security in IoT and cloud computing environments. The meticulously crafted methodology, which encompassed data preprocessing, feature engineering, dataset selection, and hyperparameter tuning, played a pivotal role in achieving these results. The careful selection of the dataset, enriched with diverse network behaviors, provided a robust foundation for the predictive model. Feature engineering, guided by domain knowledge, allowed us to capture unique characteristics of IoT botnet attacks, thereby enhancing the model's predictive capabilities. Furthermore, the comparative analysis highlighted the superiority of the proposed VAE model in key performance metrics compared to prior research endeavors, demonstrating the innovation and efficacy of the approach in addressing IoT security challenges. In the realm of IoT, where the proliferation of connected devices continues unabated, the research contributes a foundational piece to the security puzzle. The proposed VAE-based model not only bolsters defenses against botnet attacks but also lays the groundwork for future advancements in data transmission security.

Several promising avenues for further exploration emerge from this research. Firstly, continued refinement of the VAE-based model can lead to even higher accuracy and precision, making it an indispensable tool in defending against IoT botnet attacks. Additionally, the principles and techniques developed here can be adapted to enhance security in various other domains, including network security, anomaly detection, and intrusion prevention. Collaboration with industry partners to implement and deploy this predictive model in real-world IoT and cloud computing environments is another exciting prospect. This can provide valuable insights into the model's performance in practical scenarios. Furthermore, as the IoT ecosystem continues to evolve, new types of threats and attack vectors may emerge. Research in adapting and evolving the predictive model to counter these evolving threats will be crucial. Therefore, this research serves as a significant contribution to the ongoing efforts to secure IoT and cloud computing environments. Implementing the predictive model in cloud and IoT environments enables proactive monitoring, anticipating botnet attacks for early detection and mitigation. Leveraging Variational Autoencoders (VAEs), the model can identify nuanced patterns related to emerging threats, enhancing defense in the dynamic IoT and cloud landscape. Future improvements may involve seamless integration with existing security systems, collaborating with intrusion detection systems, firewalls, and other measures for a comprehensive defense strategy.

Acknowledgements

The author would like to appreciate the effort of the editors and reviewers. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author contributions

All authors are equally contributed.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] R. Daws, 'Asimily Report Highlights Threats to Connected Healthcare Devices.' Internet of Things News. IoT Tech *News*, August 23, 2023. Available at: https://www.iottechnews.com/news/2023/aug/23/asimily-report-threats-connected-healthcare-devices/.

[2] R. Daws, "'Enterprises Accelerate IoT Deployments to Drive Digital Transformation.' Internet of things news. IoT tech *News*, August 15, 2023". Available at: https://www.iottechnews.com/news/2023/aug/15/enterprises-accelerate-iot-deployments-digital-transformation/.

[3] R. Daws, "'Qiang Huang, Palo Alto Networks: On Addressing IoT Device Security Challenges.' Internet of things news. IoT tech *News*, August 16, 2023". Available at: https://www.iottechnews.com/news/2023/aug/16/qiang-huang-palo-alto-networks-iot-device-security-challenges/.

[4] R. Daws, "'Kaleido Intelligence Forecasts ESIM Adoption Surge for IoT.' Internet of things news. IoT tech *News*, August 21, 2023". Available at: https://www.iottechnews.com/news/2023/aug/21/kaleido-intelligence-forecasts-esim-adoption-surge-iot/.

[5] R. Daws, "'Z-Wave Alliance Celebrates Trident IoT's Launch.' Internet of things news. IoT tech *News*, August 17, 2023". Available at: https://www.iottechnews.com/news/2023/aug/17/z-wave-alliance-celebrates-trident-iot-launch/.

[6] B. Bojarajulu et al., "Intelligent IoT-BOTNET attack detection model with optimized hybrid classification model," *Comput. Sec.*, vol. 126, no. 103064 (2023), p. 103064, Mar.2023.

[7] S. Khanam et al., "Towards an effective intrusion detection model using focal loss variational AutoEncoder for Internet of things (IoT)," *Sensors (Basel, Switzerland)*, vol. 22, no. 15, p. 5822, Aug. 2022.

[8] V. Gugueoth et al., "Security of Internet of things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects," *ICT Express*, vol. 9, no. 5, pp. 941-960, Oct. 2023.

[9] H. Lin et al., "Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine," *Digit. Commun. Netw.*, vol. 9, no. 1, pp. 111-124, Feb. 2023.

[10] Q. Abu Al-Haija and M. Al-Dala'ien, "ELBA-IoT: An ensemble learning model for botnet attack detection in IoT networks," *J. Sens. Actuator Netw.*, vol. 11, no. 1, p. 18, Mar. 2022.

[11] L. Tan et al., "A new framework for DDoS attack detection and defense in SDN environment," *IEEE Access Pract. Innov. Open Solut.*, vol. 8, pp. 161908-161919, Sep.2020.
[12] O. Jullian et al., "Deep-learning based detection for cyber-attacks in IoT networks: A distributed attack detection framework," *J. Netw. Syst. Manag.*, vol. 31, no. 2, Feb. 2023.
[13] S. Garg et al., "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks," *IEEE Trans. Netw. Serv. Manage.*, vol. 16, no. 3, pp. 924-935, Jul.2019.
[14] A. A. Nancy et al., "IoT-cloud-based smart healthcare monitoring system for heart disease prediction via deep learning," *Electronics*, vol. 11, no. 15, p. 2292, Jul. 2022.
[15] V. Gugueoth et al., "Security of Internet of things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects," *ICT Express*, vol. 9, no. 5, pp. 941-960, Oct. 2023.
[16] B. Kolosnjaji et al., "Deep learning for classification of malware system call sequences" in *AI 2016, Adv. Artif. Intell.* Cham: Springer International Publishing, pp. 137-149, Nov.2016.
[17] D. Ingle and D. Ingle, "An enhanced blockchain based security and attack detection using transformer in IOT-cloud network," *ARASET*, vol. 31, no. 2, pp. 142-156, Jul.2023
[18] V. A. Devi et al., "Reliable and secure data transfer in IoT networks using knight-tour and PHLSB method," *ARASET*, vol. 32, no. 2, pp. 107-118, Oct. 2023.
[19] "UNSW_NB15," *Kaggle: Your Machine Learning and Data Science Community*. Available at: https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15.
[20] A. Asperti and M. Trentin, "Balancing reconstruction error and Kullback–Leibler divergence in variational autoencoders," *IEEE Access Pract. Innov. Open Solut.*, vol. 8, pp. 199440-199448, Oct. 2020.
[21] "Kullback–Leibler divergence," *Wikipedia, The Free Encyclopedia*. last modified September 18, 2023 https://en.wikipedia.org/w/index.php?title=Kullback%E2%80%93Leibler_divergence&oldid=1175951168.
[22] "Deriving the KL divergence loss for VAEs," *Cross Validated*. Available at: https://stats.stackexchange.com/questions/318748/deriving-the-kl-divergence-loss-for-vaes.