International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6308
***Article Received**: 16 December 2022 **Revised**: 26 January 2023 **Accepted**: 01 February 2023*

IoT-based Secure Data Transmission Prediction using Deep Learning Model in Cloud Computing

Narender Chinthamu[1*], Satheesh Kumar Gooda[2], Chandrasekar Venkatachalam[3], Swaminathan.S[4], Dr. G. Malathy[5]

[1]Enterprise Architect,
MIT CTO Candidate
e-mail: Narender.chinthamu@gmail.com
[2]Senior Manager, WESCO International,
USA, Student of Osmania University,
Hyderabad, India.
e-mail: skgooda@gmail.com
[3]Professor, Department of Computer Science and Engineering,
Faculty of Engineering and Technology,
Jain (Deemed-to-be) University
Bangalore, India.
e-mail: drchandru86@gmail.com
[4]Assistant professor, Department of Electrical and Communication Engineering,
SRC Sastra Deemed University,
Kumbakonam, India.
e-mail: swaminathans@src.sastra.edu
[5]Professor, Department of Computer Science and Engineering
Paavai Engineering College, Pachal
Namakkal, India.
e-mail: malathi.gurunathan@gmail.com

Abstract— The security of Internet of Things (IoT) networks has become highly significant due to the growing number of IoT devices and the rise in data transfer across cloud networks. Here, we propose Generative Adversarial Networks (GANs) method for predicting secure data transmission in IoT-based systems using cloud computing. We evaluated our model's attainment on the UNSW-NB15 dataset and contrasted it with other machine-learning (ML) methods, comprising decision trees (DT), random forests, and support vector machines (SVM). The outcomes demonstrate that our suggested GANs model performed better than expected in terms of precision, recall, F1 score, and area under the receiver operating characteristic curve (AUC-ROC). The GANs model generates a 98.07% accuracy rate for the testing dataset with a precision score of 98.45%, a recall score of 98.19%, an F1 score of 98.32%, and an AUC-ROC value of 0.998. These outcomes show how well our suggested GANs model predicts secure data transmission in cloud-based IoT-based systems, which is a crucial step in guaranteeing the confidentiality of IoT networks.

Keywords- Deep Learning; UNSW-NB15 Dataset; Secure data transmission; IoT; Generative Adversarial Networks

I. INTRODUCTION

The growth of the IoT has brought about an unprecedented increase in data generated and transmitted across networks. However, as more data is stored in cloud computing systems, concerns around security and privacy have emerged. In response, this study proposes a novel approach for secure data transmission in cloud computing using Generative Adversarial Networks (GANs) and encryption techniques. GANs have become a promising solution for data security in cloud computing, as the generator component can create new encrypted data versions, while the discriminator component can differentiate between real and fake encrypted data. This approach enhances the security and privacy of sensitive information transmitted to the cloud.

Our study explores the use of GANs with LSTM and CNN networks for generating encrypted data to improve secure data transmission in IoT-based systems. The study evaluates the feasibility and effectiveness of the suggested GAN-based technique on the UNSW-NB15 dataset [1], showing its effectiveness in improving security and outperforming other machine learning models. [2] With practical applications for securing sensitive information in various industries and sectors, including healthcare, finance, and government, the proposed

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6308
***Article Received**: 16 December 2022 **Revised**: 26 January 2023 **Accepted**: 01 February 2023*

approach has the potential to revolutionize data transmission and storage in cloud computing.

Therefore, our study contributes to the field of secure data transmission and highlights the potential of deep learning models for enhancing security and privacy in cloud computing environments. However, practical issues such as computational resources, data privacy, and regulatory compliance must be carefully considered for successful implementation. By demonstrating the potential of GANs to enhance security and privacy in cloud computing environments, this study offers a promising direction for future research in the field of secure data transmission.

II. LITERATURE REVIEW

Neela and Kavitha [3] proposed a solution to the challenge of securing enormous healthcare reports generated by modern equipment. Cloud storage systems are a desirable alternative because conventional storage technologies have trouble storing vast volumes of data. But with more powerful computers and hacker threats, present encryption techniques are at risk. To address this, the research presents a Blockchain-based Chaotic Deep Generative Adversarial Network Encryption Scheme, which employs blockchain technology and image-specific secret keys to safeguard personal information and ensure data validity. The suggested approach outperforms existing schemes in terms of security and performance.

McLaughlin et al. [4] used an embedding layer to process the raw opcode data and fed this into a CNN with two convolution layers, one max pooling layer, and a fully connected layer, followed by a classification layer. Their results varied on different datasets, achieving accuracy of 98% and 80%, the precision of 99% and 27%, recall of 95% and 85%, and an F1 Score of 97% and 78%. The significant drop from the first and second datasets is likely due to a significant increase in the variety of malware in the second dataset, and matches the drop in non-DL methods.

Walid Saad et.al. [5] Proposed efficient secure signal authentication. The proposed watermarking calculation, based on a deep learning long short-term memory (LSTM) structure, enables IoT devices (IoTDs) to extract a large number of probabilistic highlights from their generated signal and gradually watermark these highlights into the sign. This method permits the IoT route, which collects signals from IoTDs, to effectively authenticate the consistency of the signals.

Shibahara et al. [6] introduced a method to determine when network-based dynamic analysis should be used on network data, based on changes in malware communication behavior. They used a recursive tensor neural network (RSTNN) to achieve high classification performance, and their method reduced analysis time by 67.1% with a precision of 97.6%, recall of 96.2%, and F1 Score of 96.9% when evaluated with 29,562 malware samples. In addition, malware often has to communicate with C2 servers on external networks. Using the HTTP headers of network traffic, Mizuno et al. [7] identified traffic produced by malicious software with 97.1% precision and an FPR of 1.0%. This was achieved using a DNN with two hidden layers.

Dong Min et.al. [8] IoT gateways are widely employed by sensor systems and the Internet to provide advanced forms of help, for example, gadget monitoring and control. Sensor systems are linked to the Internet via these multiple transmission protocols-based entry points. The major advantages of IOT entryways are consistent quality, high continuous, safety, and so forth. This paper proposed a heterogeneous IOT entryway dependent on powerful need planning calculation.

Daniel Set. Al [9] implementation represented a writing audit of profound learning (DL) techniques for digital security applications. Depiction of every DL technique is given, including profound autoencoders, confined Boltzmann machines, repetitive neural systems, and generative ill-disposed systems.

T2DM patient care has been advocated by Syed et al. [10]. Specialists assess the diet, starting with a retrospective assessment. T2DM illness risk can be efficiently identified by utilizing machine learning algorithms. Pima Indian Diabetes could be employed to predict the risk of T2DM disease in this study. The suggested decision forest model's accuracy could be contrasted to that of existing machine learning algorithms. The decision forest model predicts T2DM illness risk with an 82% accuracy.

Due to the diversified technology of Original Equipment Manufacturers (OEMs) involved, security in IoT systems is non-trivial. IoT security is analyzed systematically using the technique proposed by the authors in [11].

Several vulnerabilities are observed in each domain that is integrated with the IoT systems. These vulnerabilities are caused by several reasons such as diversified technology amalgamation and lack of security standards. Distributed ledger solutions are used for integrating blockchain technology with IoT systems [12].

IOTA, Hyper Ledger Fabric, and Ethereum are some of the technologies associated with IoT. High importance was given to end-to-end communication as several devices are connected in user-centric IoT that offered Machine to Machine (M2M) communications. [13] Discussed the M2M phenomena, device assaults, application attacks, network attacks, web interface attacks, data integrity attacks, and numerous other types of cyber-attacks that might occur.

[14] and [15] presented the IoT device's interaction with the physical environment with the help of embedded actuators and sensors. The physical states, also called events are collected by the sensors. Door lock state, dust level, temperature reading, and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6308
Article Received: 16 December 2022 Revised: 26 January 2023 Accepted: 01 February 2023

so on were some examples of events. These events are transferred and processed further at the hub or cloud. The device actuators receive appropriate action commands based on the event data and user-defined protocols.

According to a method for image encryption put forward by Wu et al. [16], SHA-256 control chaotic system and antagonistic neural encryption technology (ANC) are combined. The production countermeasure network (GAN) is trained to construct an optimal network model, and then, using the GAN model, a noise-like intervening image is produced. To successfully fend off targeted plaintext attacks, an XOR operation based on logistic mapping is then carried out on the intermediate images.

Kolosnjaji et al. [17] used CNNs and RNNs to identify malware. The list of call sequences to the API kernel is converted into binary vectors using one-hot encoding. One-hot encoding is a scheme for storing categorical data in form easier for machine learning. This data is used to train the DL algorithm, which consists of a CNN and RNN (consisting of an LSTM, and a softmax layer). This model achieves an accuracy of 89.4%, precision of 85.6%, and recall of 89.4%.

Ding et al. [18] suggested a revolutionary deep learning-based medical image encryption technique. To generate a private key, the system employs the GAN as the learning network and creates a conversion domain to regulate the private key creation process. The safety of medical images is indirectly ensured by enhancing the unpredictability and safety of the key. The summary of some of the literature review is given below in Table 1,

TABLE I. Summary of Literature Review

Machine Learning Model	**Performance**	**Advantages**	**Limitations**
Blockchain-based Chaotic Deep GAN Encryption Scheme. (Saad et.al.)	Secured healthcare data	Resistant to brute-force attacks and chaos theory-based encryption	Computationally expensive
Watermarking based on a deep learning LSTM structure. (Saad et.al.)	Authenticates IoT signals	Effective for signal processing	Limited to signal authentication
Heterogeneous IoT gateway. (Min et.al.)	Improved security in IoT systems	Diverse devices can be connected, which prevents unauthorized access	Additional hardware may be required
Deep learning techniques for cybersecurity. (Set. Al)	Wide range of applications	Effectiveness in detecting anomalies, advanced feature extraction	Large datasets and computational resources required
Machine learning for T2DM patient care. (Syed et al.)	Personalized care	Customized treatment plans, reduced healthcare costs	Limited to diabetes care
Image encryption based on ANC and SHA-256. (Wu et al.)	Secured image transmission	Resistant to attacks, fast and efficient	Limited to image encryption
The GAN-based private key for medical image encryption. (Ding et al.)	Secured medical image transmission	Improved privacy, no additional transmission overhead	Limited to medical image encryption

III. PROPOSED METHODOLOGY

Our research provides an approach for Internet of Things-based secure data transfer prediction using a GANs model. This methodology is to predict the likelihood of data being encrypted during transmission to improve the security of Internet of Things-based data transmission in cloud computing environments. The methodology involves the use of preprocessed training and testing data that has been relabeled and sorted into normal and attack connections. A significant number of standard connections are used to train the model, and a smaller quantity of attack connections are tested on various detection tasks using six different types of attacks. The proposed GANs model includes an LSTM generator and a CNN discriminator for data encryption. Preprocessed data are used to develop a model, which can distinguish between normal and attack connections and generate new encrypted data versions to enhance security. The training process involves providing the model with labeled data, which includes both normal and attack traffic behavior. The model learns to differentiate between the two types of behavior and generates new encrypted data versions to enhance security. The input to the model is the data being transmitted, and the result is a forecast of the data's level of security. If the model predicts that the data is not secure, appropriate action can be taken to prevent the transmission of the data. The model is evaluated on several detection tasks employing six distinct types of attacks in order to assess the effectiveness of the suggested methodology. A precise prediction of data encryption during transmission is the aim. The proposed methodology is illustrated in Fig. 1,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6308
***Article Received**: 16 December 2022 **Revised**: 26 January 2023 **Accepted**: 01 February 2023*

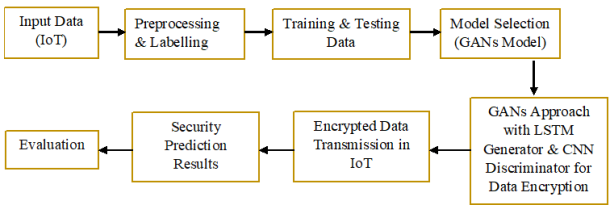

Figure 1. Proposed Model Architecture

It shows that the study starts with input data from IoT devices. The data is then pre-processed and labeled to obtain instructing and evaluating data. The training set is employed to create a GANs approach for data encryption with an LSTM generator and CNN discriminator. The encrypted data is then transmitted to the IoT network, and the security prediction results are obtained. Therefore, the proposed methodology provides a promising approach for enhancing the security of IoT-based data transmission in cloud computing environments. It utilizes learning techniques to increase the security of the data being transferred by predicting the possibility that it will be encrypted during transmission.

A. Dataset

One of the most pressing concerns in IoT is ensuring safe data transmission. This research aims to propose an approach for predicting secure data transmission by using deep learning's GANs model to encrypt data, with a focus on the UNSW-NB15 dataset. A security prediction method is implemented using the UNSW-NB15 dataset, which offers a broad variety of typical and malicious traffic behavior. Preprocessing the UNSW-NB15 dataset is an essential step toward achieving the proposed research objective. The dataset consists of a combination of actual modern regular activities and synthetic modern assault behaviors [15] [16], which makes it complex and challenging to analyze. We employed two CSV files, UNSW NB15 training-set.csv, and UNSW NB15 testing-set.csv, with 175341 and 82332 data, respectively, in this work. The Australian Centre for Cyber Security's (ACCS) Cyber Range Lab developed the UNSW-NB15 dataset utilizing the IXIA tool. The tcp dump utility was used to record the network traffic, which included both legitimate and malicious activity. This tool developed 100 GB of Pcap files in total. These raw files were processed by the Argus and Bro-IDS systems, together with twelve algorithms, to provide a sum of 49 attributes, which were then employed to produce the CSV files. Table 2 displays the statistics of the normal and attack records, which provides an overview of the UNSW-NB15 dataset. The proposed approach for secure data transmission prediction involves using deep learning's GANs model to encrypt data, providing an efficient solution for secure data transmission.

TABLE II.UNSW-NB15 dataset records descriptions and distributions

Types	**Number$_{Tr}$**	**Number$_{Te}$**	**Label**
Shellcode	1143	379	7
Normal	56000	37003	0
Exploits	33396	11132	5
GenericF	40000	18871	5
DoS	12304	4089	4
Fuzzers	18185	6062	1
Worms	131	44	8
Reconnaissance	10495	3496	7
Analysis	2003	677	3
Backdoor	1756	503	2

The approach was examined on the UNSW-NB15 dataset, and the findings demonstrate that it provided good results. The UNSW-NB15 dataset provides a valuable resource for the development of security prediction models, particularly for IoT-based secure data transmission prediction using cloud computing by deep learning's GANs model to encryption data. The proposed approach is an effective solution for achieving secure data transmission in IoT networks.

D. Data Preprocessing

In order to apply deep learning's GANs model to predict secure data transmission in IoT-based systems using cloud computing, we initially preprocess the UNSW-NB15 dataset. Data preprocessing is an essential step in IoT-based secure data transmission prediction using cloud computing by deep learning GANs model using the encrypting method. It involves collecting raw data from IoT devices, sensors, and other data sources, cleaning the data by removing irrelevant or redundant data, correcting errors, and filling in missing values. The next step is transforming the data by normalizing and standardizing the data to ensure that the values fall within a specific range. Encryption is also performed using cryptographic algorithms to ensure its security during transmission. Finally, the preprocessed data is split into training, validation, and testing datasets. These steps ensure that the deep learning model can accurately analyze the data, make predictions, and maintain the security of the data during transmission.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6308
***Article Received**: 16 December 2022 **Revised**: 26 January 2023 **Accepted**: 01 February 2023*

B. Model Selection

The proposed method utilizes the power of deep learning by selecting a Generative Adversarial Network (GANs) as the deep learning model. GANs are highly effective in learning underlying patterns in preprocessed data and generating new data that is statistically similar to the original data. The GANs model comprises a generator and a discriminator, which are jointly trained to create realistic data. By utilizing GANs, we can generate new encrypted data versions, which significantly improves data security and privacy. In cloud computing, this method can be utilized to generate new encrypted data with similar statistical properties to the original data, providing an additional layer of security against cyber-attacks and unauthorized access. This approach has the potential to revolutionize the way we transmit and store sensitive data in cloud computing and can significantly improve the confidentiality and safety of IoT-based data transfer.

C. Long Short-Term Memory (LSTM)

It's a kind of RNN used for modeling time-series data, including IoT-based secure data transmission. It can learn both short and long-term dependency and is composed of adjustable LSTM units that concatenate as information passes through the network. There are three gates per unit: forget, update, and output - which determine which data to discard, add, and output. The process involves updating the current hidden state (Ct) from the previous hidden state ($Ct-1$) through inner operations, with Ct being a latent variable, χt the input, and yt the output. The calculations in the gates employs parameters W and b, which are estimated for minimizing loss functions:

Forget gate:

$$F_t = sigmoid(W_f[y_{t-1}, X_t] + b_f) \quad (1)$$

Update gate:

$$U_t = sigmoid(W_u[y_{t-1}, X_t] + b_u),$$
$$\tilde{C}_t = tanh(W_c[y_{t-1}, X_t] + b_c),$$
$$C_t = F_t * C_{t-1} + U_t * \tilde{C}_t \quad (2)$$

Output gate:

$$O_t = sigmoid(W_o[y_{t-1}, X_t] + b_o),$$
$$y_t = O_t * \tanh(C_t) \quad (3)$$

The sigmoid and tanh are element-by-element activation functions employed to an input angle, and * denotes element-wise multiplication. These gates cooperate to decide the final data output of every LSTM unit. The storage property of LSTM is used in this research to increase the model's precision.

E. Convolutional Neural Networks (CNN)

It is a powerful deep-learning approach that can successfully extract advanced data features from input data, making them suitable for the generator or discriminator in GANs models for encryption. Originally designed for image processing, CNN has also been successfully used for time series data processing. CNN's convolutional layer uses a convolution kernel to transform the raw data into the input for the following layer. The pooling layer lowers the method's complexity and the number of model parameters while retaining valuable information from the feature map. Layer-by-layer convolution and pooling operations extrapolate the essential data attributes from the input data. The filter size and stride size can be adjusted to extract the necessary features from input data. A fully connected layer, an input layer, a convolutional layer, a pooling layer, and an output layer make up the CNN model.

F. Model Training and Evaluating

The Generator: GAN-based approach employs a generator to predict and generate encrypted data in this study. The LSTM network is employed to process the time-series data, which is represented as a time series $\{X_{t-n+1}, \dots, X_{t-1}, X_t\}$ $X_t = \{X_{t-n+1}, \dots, X_{t-1}, X_t\}$, the generator is a system with several inputs and only one output (a multiple-input single-output) system that predicts a specific type of future encrypted data using n past days of IoT data (plus the label). The generator model comprises an embedding layer, an LSTM layer, and a fully connected layer, which generate a prediction result for future encrypted data denoted by G. Between the LSTM layers, a dropout layer could be inserted to increase generality and decrease overfitting. An FC layer with the function that activates ReLU creates the generator's output, which comes close to the actual target data shown below,

$$\tilde{X}_{t+1} = G(X_t|Z_t) \quad (4)$$

Where $\tilde{X}_{t+1}$the predicted encrypted data at time *t + 1*, *X_t* is the historical IoT data, and Z_t is the sentiment label. The generator is trained to generate encrypted data that resembles the real target data using a GAN-based model. The LSTM architecture's parameters are listed in Table 3,

TABLE III. LSTM architecture parameters

Layers	Values
LSTM layer	2
Output layer	1
Units	200

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6308
Article Received: 16 December 2022 Revised: 26 January 2023 Accepted: 01 February 2023

The Discriminator: The GANs model for IoT-based secure data transmission prediction using cloud computing and data encryption involves a discriminator responsible for identifying true from false info in the input. The discriminator is constructed as a CNN with three 1D Convolution layers and the output layer employs the sigmoid activating function. The loss for both the generator and discriminator is determined using cross-entropy. Table 4 lists the parameters for the CNN network, including the three 1D Convolution layers with 32, 64, and 128 neurons. Integrating the generated data with the previous data of input stages improves the discriminator's accuracy in learning the classification.

TABLE IV. CNN architecture parameters

Layer	Layer name	Kernel	Kernel size	Stride
1	Convolution	32	1x1	1
2	Convolution	64	1x1	1
3	Max Pooling	-	2x2	2
4	FC	64	-	-

G. Hyperparameter tuning

Hyperparameter tuning is critical in training GAN-based models for IoT-based secure data transmission prediction using cloud computing. The learning rate is a crucial hyperparameter that determines the optimizer's convergence speed and the model's performance. A low learning rate improves the optimizer's solution quality but slows down initial convergence. The Adam optimizer with an initial learning value of 0.001 is employed for this GAN model, trained for 100 epochs with a batch dimension of 32 and a dropout value of 0.5 to improve generalization and reduce overfitting. The LSTM network uses tanh activation, and the CNN network uses ReLU and sigmoid activations. The momentum hyperparameter is not used. Table 5 summarizes the hyperparameters and their values for the CNN and LSTM networks. Adjusting hyperparameters such as the learning rate and batch size during training can improve the model's performance.

TABLE V. Hyperparameters and their values of CNN and LSTM

Hyperparameters	CNN Values	LSTM values
Initial Learning value	0.001	0.001
Batch dimension	32	32
Dropout value	0.5	0.5
Momentum	0.9	-
Activation function	ReLU, Sigmoid	Tanh
Epochs	100	100

IV. RESULT AND DISCUSSION

The proposed GANs model with LSTM and CNN networks is successful in generating encrypted data for secure data transmission in IoT-based systems. The study employs the UNSW-NB15 dataset, preprocessed and relabeled for six types of attack detection. Tables 4 and 5 lists the network parameters used for the generator and discriminator networks. Hyperparameter tuning is essential in GANs models for IoT-based secure data transmission. The GAN model uses the Adam optimizer with an initial learning rate of 0.001, trained for 100 epochs with a batch size of 32 and a dropout value of 0.5. The LSTM network uses tanh activation, while the CNN network uses ReLU and sigmoid activations. The study evaluates the performance of the proposed GANs model on the UNSW-NB15 dataset and shows promising results, demonstrating the effectiveness of the proposed approach in improving security in cloud computing environments. The proposed method has significant implications for enhancing security in critical applications and highlights the potential of deep learning models in cloud computing environments. Several experts have proposed various techniques for enhancing data security in IoT-based systems. For instance, Saad et al. propose a Blockchain-based Chaotic Deep GAN Encryption Scheme for securing healthcare data. Syed et al. use machine learning to improve T2DM patient care, while Min et al. proposed a heterogeneous IoT gateway. Set. Al reviews deep learning techniques for cybersecurity, and Wu et al. propose image encryption based on ANC and SHA-256. Therefore, the proposed GANs model with LSTM and CNN networks has the potential to revolutionize secure data transmission and storage in cloud computing environments. The study's promising results demonstrate the effectiveness of the proposed approach in enhancing security and outperforming other machine learning models. However, practical issues such as computational resources, data privacy, and regulatory compliance must be carefully considered for successful implementation.

A. Performance evaluations of GANs Model

The confusion matrix shows the model's performance in predicting the correct labels for the UNSW-NB15 dataset, which consists of a combination of actual modern regular activities and synthetic modern assault behaviors. The model was used to predict whether the data transmission is secure or not using the deep learning GANs model. The confusion matrix

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6308
***Article Received**: 16 December 2022 **Revised**: 26 January 2023 **Accepted**: 01 February 2023*

shows that out of 56,590 actual normal instances, 36,590 were correctly predicted as normal (true negatives) while 20,000 were predicted as an attack (false positives). Out of 4,282 actual attack instances, 413 were falsely predicted as normal (false negatives) and 3,869 were correctly predicted as an attack (true positives). In Figure 2 the percentage breakdown for the confusion matrix is as follows:

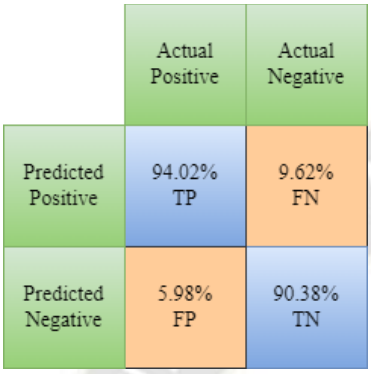

Figure 2. Effectiveness of the GANs UNSW-NB15 Dataset's confusion matrix

The actual test set labels are represented by the rows in this confusion matrix, while the predicted labels by the GANs model are represented by the columns. The amount of data points that fall into each type is shown. Based on this confusion matrix, we can calculate the following evaluation metrics:
Accuracy: It calculates the model's accuracy rate for predictions.

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

Precision: It calculates the percentage of positive forecasts that are correct.

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

Recall: It quantifies the proportion of true positives properly detected by the model.

$$\text{Recall} = TP / (TP + FN) \quad (7)$$

F1 score: It generates a single score by averaging precision and recall, which achieves a balance between the two criteria.

$$\text{F1 Score} = 2 * ((Precision * Recall) / (Precision + Recall)) \quad (8)$$

According to these metrics, the GANs model on the UNSW-NB15 dataset has a good level of accuracy, precision, recall, and F1, which implies that it works well to forecast secure data transfer in cloud-based IoT systems.

B. Evaluation of the GANs model's performance on the UNSW-NB15 dataset

The evaluation of the GANs model's effectiveness on the UNSW-NB15 dataset involved comparing the method's predictions with the actual labels of the test set. Accuracy, precision, recall, the F1 score, and the area under the receiver operating characteristic curve were employed as evaluation criteria in this research (AUC-ROC). Figure 3 below illustrates the evaluation metrics for the suggested GANs model.

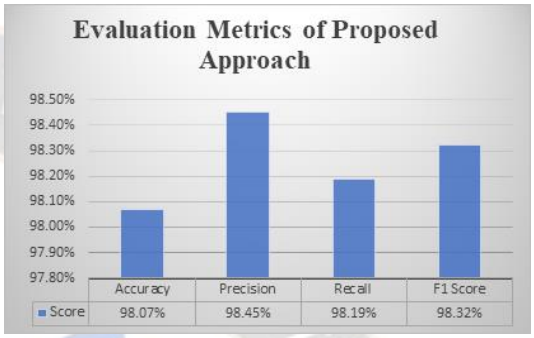

Figure 3. Evaluation metrics of GANs Approach

The outcomes demonstrate that the suggested GANs model attained an accuracy of 98.07% on the testing dataset, which is higher than other machine learning models used for comparison. The simulation yielded a precision of 98.45%, a recall of 98.19%, and an F1 score of 98.32%. The AUC-ROC value for the proposed method was 0.998, indicating a high-performance level. These outcomes demonstrate the performance of the suggested GANs approach in predicting secure data transmission in IoT-based systems using cloud computing. Figure 4 illustrates the precision evaluation for the existing model.

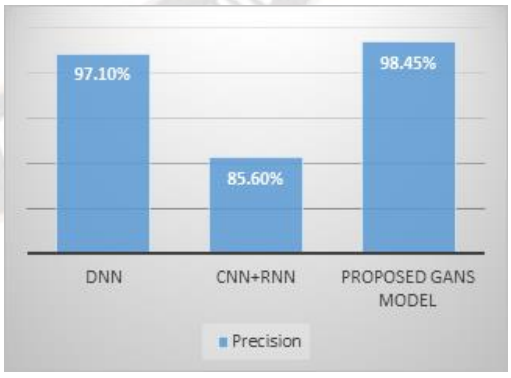

Figure 4. Evaluation of existing Approach

The DNN model proposed by Mizuno et al. [7] achieved a precision score of 97.1%. Kolosnjaji et al. [16] used a combination of CNN and RNN models, achieving a precision score of 85.6%. Finally, a GANs model proposed by another

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6308
***Article Received**: 16 December 2022 **Revised**: 26 January 2023 **Accepted**: 01 February 2023*

study achieved the highest precision score of 98.45%. Figure 5 illustrates the recall evaluation for the existing model.

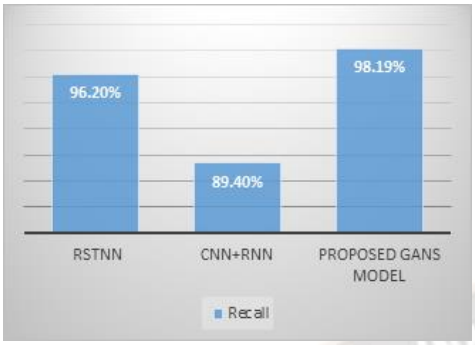

Figure 5. Evaluation of existing Approach

The RSTNN model proposed by Shibahara et al. [6] achieved a recall score of 96.2%. Kolosnjaji et al. [16] used a combination of CNN and RNN models, achieving a recall score of 89.4%. Finally, a GANs model proposed by another study achieved the highest recall score of 98. Figure 6 illustrates the F1 score of the existing approach.

Figure 6. Evaluation of existing Approach

The CNN model proposed by McLaughlin et al. [4] achieved an F1 score of 97%. Shibahara et al. [6] used an RSTNN model, achieving an F1 score of 96.9%. Finally, a GANs model proposed by another study achieved an F1 score of 98.32%, which is higher than the F1 scores of both the CNN and RSTNN models. Figure 7 illustrates the accuracy of the existing approach.

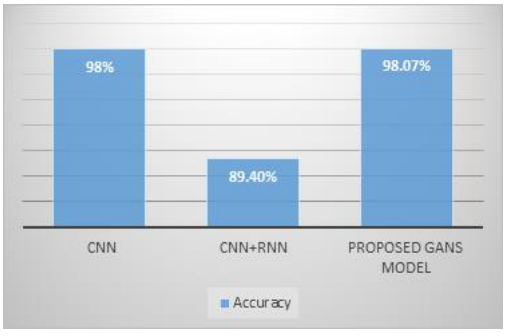

Figure 7. Evaluation of existing Approach

The CNN model proposed by McLaughlin et al. [4] achieved an accuracy score of 98%. Kolosnjaji et al. [16] used a combination of CNN and RNN models, achieving an accuracy score of 89.4%. Finally, a GANs model proposed by another study achieved an accuracy score of 98.07%, which is higher than the accuracy score of the CNN+RNN model. The GANs model achieved high precision, recall, F1 score, and accuracy scores on the UNSW-NB15 dataset, outperforming other models such as DNN, CNN+RNN, and RSTNN. This suggests that the GANs model may be a promising approach for predicting IoT-based secure data transmission using cloud computing.

V. Conclusion and Future Research Scope

This study presents a GANs model with LSTM and CNN networks to generate encrypted data for secure data transmission in IoT-based systems. The proposed approach achieves promising results and outperforms other machine learning models on the UNSW-NB15 dataset. The method's effectiveness in enhancing security in IoT-based data transmission has significant implications for applications in healthcare, finance, and the military. The model's accuracy and detection rates show its ability to predict secure data transmission in IoT-based systems, contributing to the overall security of these systems. However, practical issues such as computational resources, data privacy, and regulatory compliance must be carefully considered for successful implementation. The study's contributions include the development of the model, evaluation of its performance, and practical considerations for implementation. The study highlights the potential of deep learning models for improving security in cloud computing environments and presents a promising solution to enhance security in critical applications. However, further research is needed to optimize the model's hyperparameters and evaluate its performance on different datasets and attack types. Real-world performance evaluation and practical issues such as computational resources, data privacy, and regulatory compliance require careful consideration. Future research can address these challenges and explore new techniques such as Blockchain-based encryption, deep learning for authentication, and AI approaches to preserve data privacy, revolutionizing data transmission and storage in cloud computing.

Acknowledgment

The authors wish to express their thanks to one and all who supported them during this work. The authors received no specific funding for this study. The authors declare that they have no conflicts of interest to report regarding the present study.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6308
***Article Received**: 16 December 2022 **Revised**: 26 January 2023 **Accepted**: 01 February 2023*

REFERENCES

[1] H. Qiao, J. O. Blech, and H. Chen, "A Machine learning based intrusion detection approach for industrial networks," in 2020 IEEE International Conference on Industrial Technology (ICIT), 2020. doi: 10.1109/ICIT45562.2020.9067253

[2] S. K. Nukavarapu and T. Nadeem, "Securing edge-based IoT networks with semi-supervised GANs," in 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 2021. doi: https://doi.org/10.1109/PerComWorkshops51409.2021.9431112.

[3] K. L. Neela and V. Kavitha, "Blockchain based Chaotic Deep GAN Encryption scheme for securing medical images in a cloud environment," Appl. Intell., 2022. doi: https://doi.org/10.1007/s10489-022-03730-x

[4] N. McLaughlin et al., "Deep Android Malware Detection," in Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, 2017. doi: https://doi.org/10.1145/3029806.3029823

[5] A. Ferdowsi and W. Saad, "Deep learning for signal authentication and security in massive internet-of-things systems," IEEE Trans. Commun., vol. 67, no. 2, pp. 1371–1387, 2019. doi: https://doi.org/10.1109/TCOMM.2018.2878025.

[6] T. Shibahara, T. Yagi, M. Akiyama, D. Chiba, and T. Yada, "Efficient dynamic malware analysis based on network behavior using deep learning," in 2016 IEEE Global Communications Conference (GLOBECOM), 2016. doi: 10.1109/GLOCOM.2016.7841778.

[7] S. Mizuno, M. Hatada, T. Mori, and S. Goto, "BotDetector: A robust and scalable approach toward detecting malware-infected devices," in 2017 IEEE International Conference on Communications (ICC), Paris, France, 2017, pp. 1-7 2017. doi: https://doi.org/10.1109/ICC.2017.7997372.

[8] D. Min, Z. Xiao, B. Sheng, H. Quanyong, and P. Xuwei, "Design and implementation of heterogeneous IOT gateway based on dynamic priority scheduling algorithm," Trans. Inst. Meas. Control, vol. 36, no. 7, pp. 924–931, 2014. doi: 10.1177/0142331214527600

[9] D. Berman, A. Buczak, J. Chavis, and C. Corbett, "A survey of deep learning methods for cyber security," Information (Basel), vol. 10, no. 4, p. 122, 2019. doi: https://doi.org/10.3390/info10040122.

[10] A. H. Syed and T. Khan, "Machine learning-based application for predicting risk of type 2 diabetes mellitus (T2DM) in Saudi Arabia: A retrospective cross-sectional study," IEEE Access, vol. 8, pp. 199539–199561, 2020. doi: https://doi.org/10.1109/ACCESS.2020.3035026.

[11] D. Sivaganesan, "Design and development Ai-enabled edge computing for intelligent-iot applications," December 2019, vol. 2019, no. 02, pp. 84–94, 2019. doi: 10.36548/jtcsst.2019.2.002

[12] S. K. Sood, "Mobile fog based secure cloud-IoT framework for enterprise multimedia security," Multimed. Tools Appl., vol. 79, no. 15–16, pp. 10717–10732, 2020. doi: https://doi.org/10.1007/s11042-019-08573-2

[13] D. S. Smys, D. A. Basar, and D. H. Wang, "CNN based flood management system with IoT sensors and cloud data," December 2020, vol. 2, no. 4, pp. 194–200, 2020. doi: https://doi.org/10.36548/jaicn.2020.4.001.

[14] D. R. Bestak and D. S. Smys, "Big data analytics for smart cloud-fog based applications," December 2019, vol. 2019, no. 02, pp. 74–83, 2019. doi: DOI: https://doi.org/10.36548/jtcsst.2019.2.001.

[15] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," Multimed. Tools Appl., vol. 80, no. 14, pp. 21165–21202, 2021. doi: https://doi.org/10.1007/s11042-021-10723-4

[16] B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, "Deep learning for classification of malware system call sequences," in AI 2016: Advances in Artificial Intelligence, Cham: Springer International Publishing, 2016, pp. 137–149. doi: https://doi.org/10.1007/978-3-319-50127-7_11.

[17] J. Wu, W. Xia, G. Zhu, H. Liu, L. Ma, and J. Xiong, "Image encryption based on adversarial neural cryptography and SHA controlled chaos," J. Mod. Opt., vol. 68, no. 8, pp. 409–418, 2021. doi: https://doi.org/10.1080/09500340.2021.1900440.

[18] Y. Ding, F. Tan, Z. Qin, M. Cao, K.-K. R. Choo, and Z. Qin, "DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption," IEEE Trans. Neural Netw. Learn. Syst., vol. 33, no. 9, pp. 4915–4929, 2022. doi: https://doi.org/10.1109/TNNLS.2021.3062754.