Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

An Enhanced Blockchain Based Security and Attack Detection Using Transformer In IOT-Cloud Network

Darshan Ingle[1,*], Divyanka Ingle[2]

[1] Department of Information Technology, Thadomal Shahani Engineering College, Bandra, India
[2] IDOS Consultants LLP, Navi Mumbai, Maharashtra, India

ARTICLE INFO

Article history:
Received 2 April 2023
Received in revised form 20 June 2023
Accepted 30 June 2023
Available online 24 July 2023

Keywords:
Block chain; IOT; Cloud; Transformer; Deep Learning; Attack detection

ABSTRACT

The IoT (Internet of Things) encompasses numerous networks and connected devices. One of the primary concerns surrounding IoT, according to researchers and security experts, is the potential risks to privacy and cybersecurity. Deep learning offers significant capabilities for self-adjustment, self-organization, and generalization. Recognizing this, advanced deep learning algorithms are employed in this research to address the privacy and security issues plaguing the IoT landscape. To address these concerns, 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. To validate the proposed model, a publicly available dataset CSE-CIC-IDS2018 is employed. Pre-processing techniques, including feature selection using the chi-square method, are applied to refine the dataset. The transformer module then classifies the data as normal or abnormal, allowing for accurate identification of potential security breaches. To further safeguard the data and protect the privacy of users, a Fully Homomorphic Encryption (FHE) method is employed. This advanced encryption enables the encryption of categorized normal data, ensuring its confidentiality even during transmission and storage. The study's findings support IoT-cloud server security and privacy by demonstrating the effectiveness of the suggested paradigm in identifying and thwarting network threats. With detection times of 225.3 seconds, an accuracy of 99.25%, a precision of 99.53%, a recall of 99.32%, and an F1 score of 99.59%, the proposed system exhibits impressive performance. Furthermore, as the output numbers increase, the system's metrics improve, suggesting its scalability and flexibility.

1. Introduction

The IoT is the modern internet technology that enables a networking architecture to connect a large variety of devices in order to gather data and communicate with one another so that thoughtful

* *Corresponding author.*
E-mail address: ingledarshan@gmail.com

https://doi.org/10.37934/araset.31.2.142156

decisions may be taken. IoT offers apps that businesses may use to manage their assets and build profitable and cost-effective business models. The technology may also be utilized to improve mobility and transportation, which makes it a catalyst for a high-tech society. There are still a lot of security and privacy concerns tied to technology that is associated with the Internet of Things, such as challenges in setting up reliable and encrypted connections. This is because it is difficult to verify that all technological components interact securely due to their widespread distribution across the edge of the network.

One of the big concerns of the researchers and security experts stated is the risk to cybersecurity and privacy. IoT technologies weaknesses have been exposed through frequent, well-publicized cybersecurity attacks. This vulnerability is caused by the fact that the Internet of Things' interconnected networks make it possible to get information from unreliable sources and require new security measures.

IoT also includes a large number of networks and devices. Because of this, it is difficult to recognize, evaluate, and keep track of crucial elements that are necessary for security policy compliance. Finally, it can be challenging to develop trust and an acceptable degree of safe information transfer between different vertical information technology infrastructures. Users often fail to recognize the security risks until after a breach has occurred, which results in serious consequences such as the loss of crucial data." [1]

The continuous enhancement of intrusion detection technology has been caused by the progress of big data, cloud computing, and artificial intelligence. The detection of intrusions has traditionally mainly relied on machine learning techniques. The absence of labelled dataset, high overhead, and poor accuracy continue to be problems for these algorithms. So, Deep learning has been discovered to overcome those problems, it has been one of the most effective ways for analyzing threats and responding to security problems.

Deep learning stands apart from conventional machine learning approaches by not requiring the inclusion of manually crafted features. Deep learning additionally offers strong self-adaptability, self-organization, and generalization capacities. In the past year, academics have conducted a lot of study on deep learning since it can help detection systems become more effective at detecting things. Therefore, our research addresses both safety and conservation of energy in IoT using advanced deep learning techniques.

Even with the introduction of neural networks and the LSTM model, there are still a number of issues, such as the overfitting issue in CNNs (convolutional neural networks) and the cost of training LSTMs (Long Short-Term Memory) due to their higher bandwidth requirements. To tackle those difficulties transformer neural networks are introduced in by Vaswani et.al (2017) [15]. They are huge success in machine translation and text classification. In the transformer, applied input are converted into the fixed-dimension vectors form with the positional embedding as representations. The next step is feature extraction and utilizing encoders and decoders to understand the contextual connections between the inputs. Since the input characteristics have different impacts on the classification output, different weights of those feature representations are learned using the self-attention approach

The main contribution of the Proposed BC-TRANS Network is listed:

- Implementation of transformer neural network to capture the salient information of complicated behavior of during transmission of data in the IOT-cloud network.
- To propose a high security system using block chain and hash value authentication system.
- To improve the detection speed with high the accuracy rate on classification of data and reduce the false positive rate.

2. Literature Survey

Mei *et al*., [2] introduced the Unbounded and Puncturable Ciphertext-Policy Attribute-Based Encryption system with Arithmetic Span Program (UP-CP-ABE-ASP) in 2022. The objective of this solution is to streamline the process of sharing information and allow for the self-managed deletion of detailed data in IoT by leveraging cloud technology. By implementing a range of automated access controls, this approach empowers individuals who own the data through secure encryption while distributing it. Furthermore, the system incorporates an ASP framework to enable flexible sharing of data. Extensive performance testing has demonstrated that the UP-CP-ABE-ASP framework is effective and especially suited for cloud-assisted IoT applications, as well as flexibly robust in the classical paradigm.

Deng *et al*., [3] introduced a novel framework called Flexible Privacy-preserving Data Sharing (FPDS) for the integration of cloud-assisted IoT in 2022. An IoT user can utilize identity-based encryption to encrypt data before sending it to a receiver using the FPDS method. Much more crucially, the IoT user may provide a specific access policy to create a delegation certificate. Once the cloud decrypts any data that meets the access policy requirements, it can utilize the obtained credentials to generate fresh ciphertexts that can be accessed by a different recipient. This enables Internet of Things users to securely and flexibly share cloud-outsourced data. Extensive theoretical and empirical investigations validate the remarkable efficacy of this system.

Enabling data sharing with multiple users poses a challenge due to the limitation of the FPDS system, which currently allows sharing with only a single recipient.

According to Alkadi *et al*. [4], deep blockchain frameworks (DBF) with privacy- and security-oriented blockchains and smart contracts are utilized for distributed intrusion detection in IoT networks. The effectiveness of the deep learning method known as bidirectional long short-term memory (BiLSTM) is evaluated by analyzing sequential network data from the UNSW-NB15 and BoT-IoT datasets. This framework can serve as a tool for aiding decision-making, enabling fast, secure, and reliable data transmission between clients and cloud service providers.

The significant constraints of communication complexity and traffic overhead pose a considerable challenge for a collaborative Intrusion Detection System (CIDS) to effectively handle all network packets without experiencing any dropouts. In the case of a high volume of data being transmitted through the network, if it exceeds the maximum processing capacity of the IDS during real-time operations, a substantial portion of the network traffic needs to be eliminated. When converting sound and speech signals into text or phonemes, the spectrogram contains a large amount of information that cannot be retrieved and used by Rammo and Al-Hamdani [22].The spectrogram increases the recognition of the speaker's language because of this ability. The fundamental aim is to learn an audio signal's sophisticated discriminative features. To learn complex features, a CNN network architecture is employed.

In 2022, Fatani *et al*., [5] presented an effective strategy based on artificial intelligence (AI) for detecting intrusions in IoT systems using intrusion detection systems (IDS). The approach employed convolutional neural networks (CNNs) to extract pertinent features, and a unique feature selection method was developed using TSODE, which is a novel variant of the Transient search optimization (TSO) algorithm that utilizes operators from the differential evolution (DE) algorithm. To evaluate the effectiveness of the proposed strategy, it was tested on three publicly available datasets: KDDCup-99, NSL-KDD, BoT-IoT, and CICIDS-2017. The results showcased superior accuracy compared to numerous alternative methods. To deal with complex issues in cybersecurity, different methods are used by Maad *et al*., [21]. According to specific criteria, such as data volume, issue type, issue sensitivity, and decision tolerance in the solution. Deep learning techniques based on parallel

processing are very practical in big data and require complex processes. This section reviews the literature that have used deep learning techniques in intrusion, attack, and malware detection. The deep learning architectures are configured not on a local basis but on server-based systems to ensure data integrity, confidentiality, and reliability and to ensure that no unauthorized individuals can enter the system.

In 2020, Junaid *et al*., [20] described the utilization of a lightweight mechanism known as the misbehaviour detection specification in IoT-embedded Cyper physical system (CPS). This mechanism identified intruders by analyzing the improper behaviour of nodes within the network. However, rule-based systems are susceptible to exploitation by intelligent attackers.

In a study conducted in 2022, Alhabshy *et al*., [6] introduced a specialized anomaly-based intrusion detection system (IDS) called the Ensemble Multi Binary Attack Model (EMBAM). This system enables users to distinguish between normal behavior and abnormal attacks. The fundamental binary model of EMBAM utilizes a decision tree classifier with grid-search hyper parameter optimization. To assess the performance of EMBAM, eight or more advanced models were employed, and the experimental findings were analyzed using various performance indicators such as accuracy, detection rate, precision, specificity, false alarm rate, and F1-score. The findings demonstrated that the suggested technique outperformed alternative approaches on the UNSW-NB15 dataset, while exhibiting a similar pattern on the CICIDS2017 dataset.

Ravi and Shalinie [7] proposed an innovative machine learning (ML) approach called SDRK for intrusion detection. The SDRK model utilizes both unsupervised clustering methods and supervised deep neural networks (DNNs). Mechanisms for intrusion sensing and mitigation are implemented at the fog nodes, which serve as intermediaries between the IoT and cloud layers. The authors conducted tests on their proposed defenses using a testbed to evaluate their effectiveness against a data deluge (DD) attack. SDRK has a higher accuracy of 99.78% for detecting assaults, according to their evaluation using the NSL-KDD data set.

One limitation of this model is its need for retraining time when operating within a real-time, dynamic network.

Li *et al*., [8] developed the AE-IDS, an Intrusion Detection System (IDS) depends on deep learning and the random forest approach. The training process involves feature grouping and selection to construct a training set. By utilizing an auto-encoder, the model predicts outcomes after training, significantly reducing detection time and enhancing predictability. Experimental findings indicated that the suggested model outperformed conventional machine learning-based detection of intrusion methods according to simplified training, adaptable performance, and superior detecting precision.

One limitation of this approach is its failure to consider certain characteristics, such as the rate of false alarms and detections, in the current method.

Ponniah and Retnaswamy [9] introduced a novel model named MWKF-LSTM (Morlet Wavelet Kernel Function with Long Short-Term Memory) for intrusion detection in the IoT-Cloud platform. The MWKF-LSTM incorporates advanced techniques such as Differential Evaluation depending Dragonfly Algorithm (DEDFA), Enhanced Elliptical Curve Cryptography (E2CC) data encryption, optimal feature selection (FS) algorithm, and SHA-512 hashing. Simulation results on the NSL-KDD set of data showcased the superior effectiveness of the suggested research approach compared to previous approaches. The drawback is LSTM required long time to train the model in real time and the researchers used NSL-KDD which does not capture new attack.

To create a self-adjusting and independent abuse intrusion sensing mechanism, Papamartzivanos *et al*., [10] recommended employing auto-encoder approaches. A four-phase paradigm, consisting of 1) Monitoring, 2) Analyzing, 3) Planning, 4) Executing, and 5) Knowledge, is specially used to build the proposed system. The monitor phase enables the detection of any evolving event that requires the

adaptation of an intrusion sensing mechanism. The analysis phase transforms the unprocessed network traffic into network flows using network audit tools. Using a limited autoencoder, illustrations of the input data are learned during the planning stage. The execute phase includes storage goals. However, the study assesses performance using the NSLKDD and KDDCup 99 datasets. According to the findings, the fixed model's average accuracy is 59.71%, while the adaptive model's average accuracy is 77.99%.

The suggested model's limitations are evaluated using two outdated datasets, namely KDD Cup 99 and NSLKDD. One identified weakness is the model's inability to accurately differentiate between the R2L and U2R attack classes.

Yang *et al*., [11] introduced a novel approach known as Supervised Variational Auto-Encoder with Regularization (SAVAER), which distinguishes itself from standard GANs by utilizing WGAN-GP to learn the potential distribution of the initial information. By employing the SAVAER decoder, the training dataset is balanced, and the diversity of training samples is enhanced through the generation of instances representing rare and previously unidentified attacks. The effectiveness of the suggested model is evaluated using benchmark datasets, including UNSW-NB15, NSL-KDD (KDDTest+), and NSL-KDD (KDDTest-21). The experimental results conclusively demonstrate that SAVAER-DNN outperforms three other commonly used data oversampling techniques in terms of its ability to augment data.

The suggested approach has the limitation that, despite obtaining acceptable rates of detection for U2R and R2L attacks for the NSL-KDD dataset, when compared to the dataset's other attack classes, these rates remain lower. The suggested method’s performance at sensing attacks on minority classes is not accurately represented by the UNSW-NB15 dataset. IoT is one of the upcoming internet technologies that focuses on the delivery of services and adjusting the way that technologies are implemented across various communication networks[23-24].

A deep neural network (DNN) that was developed using 28 features from the NSL-KDD dataset is the suggested system by Thirimanne *et al*., [18]. The machine learning (ML) procedure is also implemented prior to passing real-time data to the trained DNN model for prediction. In this approach, scaling features and encoding categorical data come after each other. For accuracy, precision, recall, and the f1-score, the DNN obtained scores of 81%, 96%, 70%, and 81%, respectively.

The proposed model has some limitations, such as the fact that it yields acceptable detection rates for U2R and R2L assaults for the NSL-KDD dataset, but these rates are still lower than the dataset other attack classes. For the UNSW-NB15 dataset, the model effectiveness in identifying attacks on minority classes is not shown.

3. Methodology

The suggested work is fully outlined in this study. To identify suspicious data and ensure its secure transfer in IOT-Cloud storage, an overview of the proposed solution is given first.

3.1 BC-TRANS Network

The proposed model (Block chain) BC-Trans Network consists of block chain and transformer detect the abnormal data before storing the data in the cloud storage. Additionally Hash -2 is employed for verification of IOT users and the block chain model is used to store the user password and their details. The overview of the BC-Trans network is explained in the Figure 1 Maxime (2019) [13].

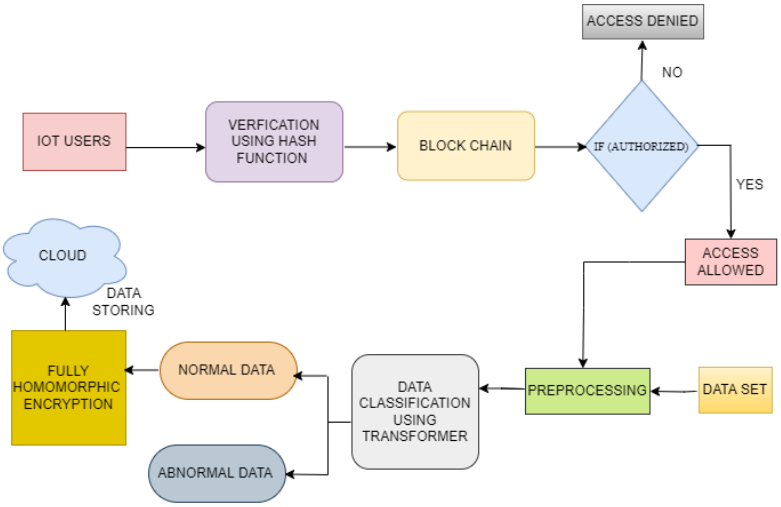

Fig. 1. Overview of the BC-TRANS system

3.2 Authentication

In the first of the proposed hash function is combined with the block chain system. The IOT users have their user Id (UD), user code number (UC) and user password (Up). They are already stored in the block chain with hash value.

When the user initiates to upload data first the request is sent to the cloud. Following receipt of the application, the cloud server delivers an authentication invocation to the block chain. Now the user will enter the data. The block chain will verify the data which are already stored with the hash function.

3.3 Verification

In the BC-TRANS Network, firstly the hash function Algorithm is combined with the block chain system. The IOT users have their user Id (UD), user code number (UC) and user password (Up). They are already stored in the block chain with hash value using SHA -2 algorithm. When the user initiates to upload data, first the request is sent to the cloud. The cloud server sends a request to the blockchain after receiving the request to validate the user's Authentication Details (AD). Now the user will enter the data, which are already stored at the time of registration'

$$HV(U_D) \oplus HV(U_C) \oplus HV(U_P) \Rightarrow Cloud\ storage \quad (1)$$

Cloud receives data in the form of Hash Value (HV) as mentioned in the Eq. 1. Now the cloud sends the AD to the Block chain server. Then the server validates the AD, if it is valid the block chain will either send a permission message to the cloud allowing the information to upload or a decline message. So, the data is kept in a secure way and there is no chance for malicious attack.

Secondly, the system is proposed to store the data in secured way with more privacy and security. The IOT devices are connected with the entry point or other edge devices data sharing, then it transmits to cloud for storing or for further processing. When exchanging data, there are several hostile assaults that might occur. In order to address this, one of the deep learning models is utilised to improve data security. Here the transformer is employed to find out the abnormal data. The publicly available dataset is collected and pre trained and then pre-processing is done.

3.4 Pre-processing

In order to improve the information capture and processing, data pre-processing requires altering the data values of a certain dataset. Therefore, the obtained dataset is initially preprocessed by carrying out specific operation such as removing redundant data and noise.

The removal of unnecessary data from the data collection is required to enhance the effectiveness and accuracy level of data mining. It is a duplicate record if there are two or more instances that represent the same entity.

Eliminating noise data is the process of removing inaccuracies from the data set that are typically present and could have an impact on the data set's actual value.

3.4.1 Feature selection

Feature selection is a method for minimizing the range of features present in a collection of data without removing crucial or pertinent information. Finding pertinent data and excluding irrelevant data are the objectives of feature selection. They are used to increase training accuracy and efficiency.

Chi-square is used to pinpoint the feature. The independence between the feature and its corresponding class label is assessed using the chi-squareX_C^2 test.

Chi-square analysis examines how far the feature O and predicted label E diverge from one another. The degree of freedom c is a measure of the power to reject the null hypothesis. The theory of autonomy should be spurned if the chi-square value is high since the class and the incidence of the feature are connected, and the feature should be used in classification research. The appropriate definition is shown in Eq. (2) [14].

$$X_C^2 = \sum \frac{(O_{i-E_i})^2}{E_i} \quad (2)$$

After the feature selection now the transformer module will classify the normal and abnormal data.

3.5 Transformer Module

The transformer is made up of position-embedded encoder and decoder blocks. In order for the model to use this information to identify the sequence's order, the transformer must first have some knowledge of the tokens' relative or absolute positions in the sequence. Therefore, "positional encodings" at the base of the encoder and decoder stacks should be included in the input embeddings.

Here, a sine function is used to encode the even places, while a cosine function is used to encode the odd positions as shown in Eq. (3) and Eq. (4).

$$PE(pos, 2i) = \sin\left(pos/1000^{2i/d_{model}}\right) \quad (3)$$
$$PE(pos, 2i+1) = \cos\left(pos/1000^{2i/d_{model}}\right) \quad (4)$$

where pos is the position and i is the dimension [15].

The data are transformed into vector forms after the position embedding. The data is subsequently processed through the encoder stack.

The encoder is a stack with N = 6 identical layers. There are two sub layers in each layer. The first is a multi-head self-focus mechanism, whereas the second is a conventional feed-forward network that is positionally fully coupled. Before layer normalization, the multi-headed self-attention layer uses a remaining connection to encircle each of the two sub-layers.

The decoder stack also has N=6 identical layers, like the encoder stack does. Following the masked multi-head self-attention layer, a residual connection, an additional normalisation layer, and a new multi-head attention layer are added (known as encoder-decoder attention). Lastly, a linear layer and a third residual connection are employed as described in the Figure 2

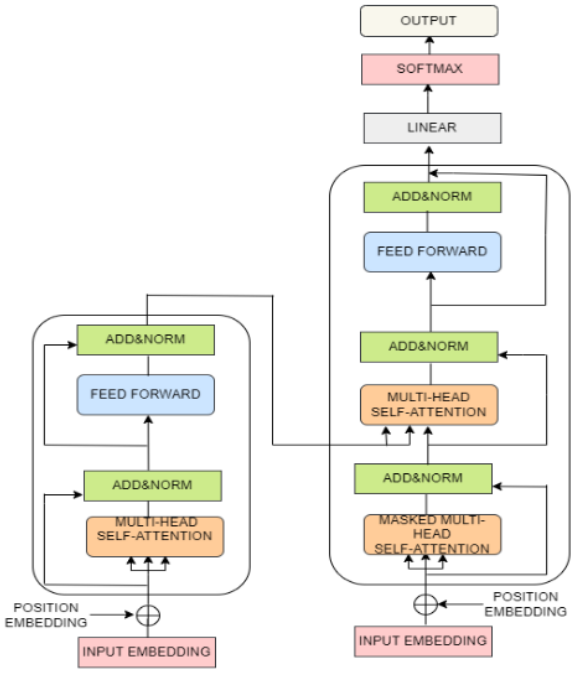

Fig. 2. Transformer module

After the masked attention layer, the normalising layer is applied to ensure that predictions for position (pos) i can only based on verified outputs at position (pos) lower than i.

A collection of queries (Q), keys (K), and values are used as input by the input attention layer (V). The model is able to simultaneously attend to data from a number of representation subspaces placed at different locations by employing multiple heads as mentioned in Figure 3. Following is the multi-head attention's final result using a concatenated computing method as stated in Eq. (5).

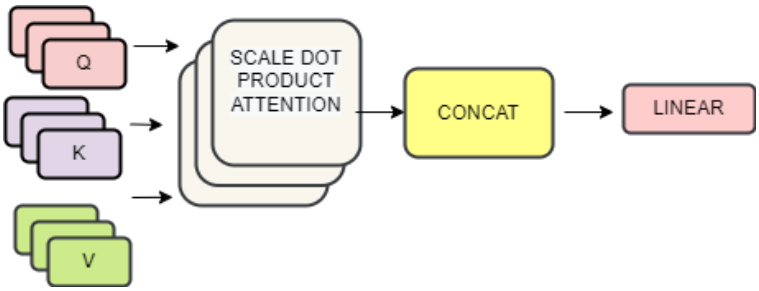

Fig. 3. The multi headed attention

$$Multihead\ (Q,K,V) = Concat(head_1 \ldots., head_a)W^0 \quad (5)$$

where h is the total number of heads. Each head must consist of:

$$Head_i = Attention\left(QW_i^Q KW_i^K VW_i^V\right) \quad (6)$$

The calculation method is similar to single-head attention, as given in Eq. (6).
where the projections are matrices of parameters $W_i^Q \in R^{dmodel \times d_k}, W_i^k \in R^{dmodel \times d_k}, W_i^v \in R^{dmodel \times d_k}, W_i^O \in R^{dmodel \times hd_k}$.

A final linear layer is utilised to convert the output, and the standard Softmax function is employed to calculate output probabilities, as mentioned in Eq. (7).

$$Attention(Q, K, V) = softmax(\frac{QK^T}{\sqrt{dk}})V \quad (7)$$

where d keys of dimension dk. The Softmax function is used to calculate the weighs on the values from the dot products of the inquiry with all of the keys, and each value is divided by $\sqrt{d_k}$.

Normal data is first categorized, and then, using a Fully homomorphic encryption method (FHE), a subgroup of intelligent encryption cryptosystems, it is encrypted. FHE allows limitless computations on the ciphertext without ever requiring its decryption or exposure. It is one of cryptography's newest generation of algorithms. When it comes to cloud computing and distributed processing, this ability is quite valuable. In practice, big data and cloud computing represent a significant implementation of completely homomorphic encryption [16]. Finally, the normal data are stored in cloud servers.

Dataset

The Canadian Institute of Cyber Security (CIC) generated the intrusion sensing dataset CSE-CIC-IDS2018 in 2018 and it is the data that is used in the BC-TRANS Network [12] Furthermore, it is the most recent and complete incursion dataset that is currently open to the public. A dataset called CSE-CIC-IDS2018 was gathered in preparation for actual attacks. Based on the CSE-CIC- IDS2017 dataset, there is an improvement.

4. Result and discussion

In order to assess performance in accordance to standard neural network rules, the CSE-CIC-IDS2018 dataset is split into two groups which are 80% training data and 20% assessing data.

Using the training dataset, models are created, and the test dataset is used to validate predictions. The SoftMax classifier distinguishes between typical and atypical data. Currently, the majority of data is classified using neural networks. With the help of the CSE-CIC-IDS2018 dataset, transformer networks are trained to more accurately distinguish between normal and abnormal input.

In this proposed work the classification is in terms of binary i.e., the malicious attacks of the network are classified in terms of normal or abnormal with four cases true positive, false positive, true negative and false negative.

4.1 Performance metrics

The performance of the proposed system is evaluated under the metrics like accuracy, precision, recall, F1score and Detection rate.

- *Accuracy*

The ratio of cases that were correctly categorized to all instances is called accuracy. As demonstrated in the following Eq. (8), it is alternatively described as the ratio of true positives (TP) and true negatives (TN) across all cases

$$ACCURACY = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

The Table 1 represents the comparison between the various model and BC-TRANS network Accuracy value

Table 1
Comparing Accuracy values with other classifiers

Classifier models	Accuracy (%)
DNN [18]	81.87
MV-FLID [19]	94.17
RTIDS [17]	98.58
BC-Trans Network	99.25

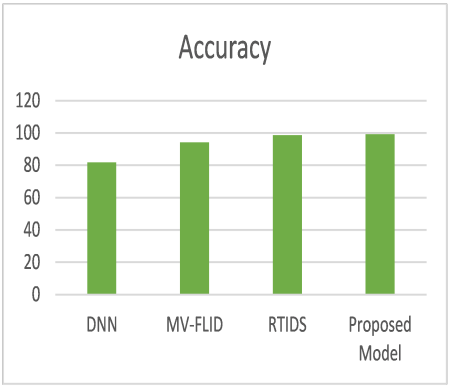

Fig. 4. Comparing Accuracy values with other classifiers

From the Figure 4 Clearly shows that accuracy value is high in comparing with the other existing methods. So abnormal data are correctly predicted and there is less chance of malicious attacks of data during the transmission.

- *Precision*

Precision is the ratio of accurately anticipated positive instances to all positively predicted instances. The precision values are tabulated and are compared with the previous classification technique in Table 2

The precision rate P of the positive class is determined by Eq. (9) as follows:

$$PRECISION = \frac{TP}{TP+FP} \quad (9)$$

Table 2
Comparing sensitivity values with other classifiers

Classifier models	Precision (%)
DNN	96.45
MV-FLID	93.26
RTIDS	98.82
BC-Trans Network	99.53

From the Figure 5, it is shown that the precision values of the BC-TRANS Network are higher than the previous method. It implies that the detection of normal data is increased and the true positive rate accuracy has been elevated.

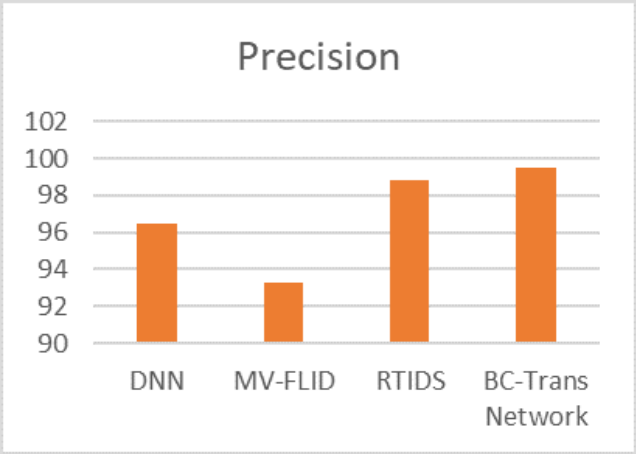

Fig. 5. Comparison of precision Value with other technique

➢ *Recall*

The proportion of correctly forecated positive events to all other occurrences in the actual class is known as recall. The other recall calculation is compared with the BC-TRANS Network and tabulated in Table 3

The recall rate R of the positive class can be calculated using Eq. (10) as shown below:

$$RECALL = \frac{TP}{TP+FN} \quad (10)$$

Table 3
Comparing Recall values with the other classifiers

Classifier models	Recall (%)
DNN	70.71
MV-FLID	93.42
RTIDS	98.66
BC-Trans Network	99.32

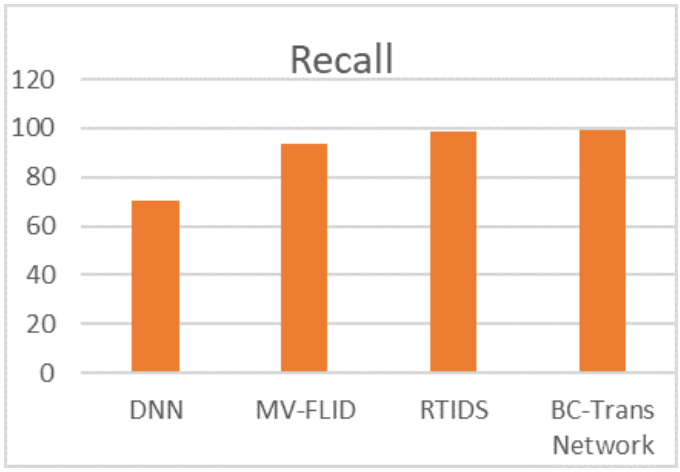

Fig. 6. Comparison of Recall Value with other techniques

From the Figure 6, it is shows that the recall values of the BC-TRANS Network are higher than the previous method. It implies that the classification of data is increased and the true positive rate accuracy is high.

- *F1 Score*

The F1 value is used to assess how a certain class affects the classification process in order to balance the accuracy rate. This score, which is calculated by averaging the precision rate and recall rate, incorporates both false positives and false negatives, as shown in Eq. (11). The F1 score values are tabulated in Table 4.

$$F1 = \frac{2 \times RECALL \times PRECISION}{RECALL + PRECISION} \tag{11}$$

Table 4
Comparing F1 score values with other classifiers

Classifier models	F1 Score
DNN	81.59
MV-FLID	94.14
RTIDS	98.48
BC-Trans Network	99.59

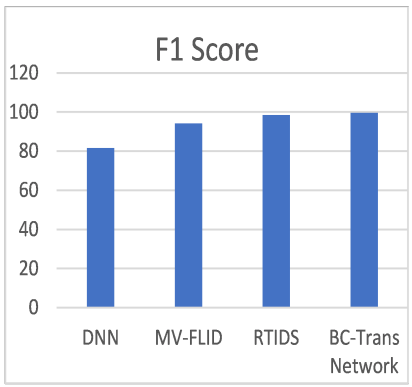

Fig. 7. Comparison of F1 score Value with other Techniques

Figure 7 shows that the proposed model has the highest F1 score when compared to the previous approach, indicating that the BC-Trans model is the most effective at categorising observations into classes.

- *Detection time*

The term detection time describes the overall amount of time required to categorise the normal and abnormal data in (sec). The detection time values are evaluated and compared with the existing methods are tabulated in the Table 5

Table 5
Comparing detection time with other classifiers

Classifier models	Detection time (sec)
DNN	315.5
MV-FLID	283.8
RTIDS	275.6
BC-Trans Network	225.3

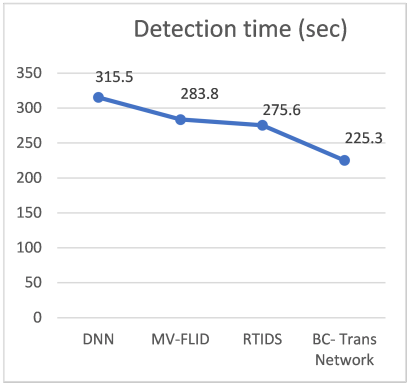

Fig. 8. Comparison of Detection time(sec) with other Techniques

From the Figure 8, the detection time for classifying the data is less in the proposed BC-Trans network in comparing with the previous model because transformer module performs parallelization so more data transmit at a time, so it predicts data in lesser time in comparing with the other existing model.

5. Conclusion

The BC-TRANS Network approach not only performed better in general but also had a higher accuracy value in the CSE-CIC-IDS2018 dataset. Machine learning and neural network-based categorization techniques make up the majority of IOT-cloud-based network malicious attack detection solutions. The proposed model results show that network attack detection is done efficiently on the transformer, as well as to improve the security and privacy in the IOT-cloud server. Additionally, Authentication via the block chain system used in the proposed model makes the network safer. As output values rise, the proposed system obtains accuracy values of 99.25%, precision levels of 99.53%, recall values of 99.32%, F1 score values of 99.59%, and detection time of 225.3 seconds, all of which are improved.

Acknowledgement
The authors extend their gratitude to everyone who provided support throughout this research. The study did not receive any dedicated funding. The authors affirm that they have no competing interests to disclose concerning the current investigation.

References

[1] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. "IoT Privacy and security: Challenges and solutions." *Applied Sciences* 10, no. 12 (2020): 4102. https://doi.org/10.3390/app10124102

[2] Mei, Qian, Minghao Yang, Jinhao Chen, Lili Wang, and Hu Xiong. "Expressive Data Sharing and Self-Controlled Fine-Grained Data Deletion in Cloud-Assisted IoT." *IEEE Transactions on Dependable and Secure Computing* (2022). https://doi.org/10.1109/TDSC.2022.3188740

[3] Deng, Hua, Zheng Qin, Letian Sha, and Hui Yin. "A flexible privacy-preserving data sharing scheme in cloud-assisted IoT." *IEEE Internet of Things Journal* 7, no. 12 (2020): 11601-11611. https://doi.org/10.1109/JIOT.2020.2999350

[4] Alkadi, Osama, Nour Moustafa, Benjamin Turnbull, and Kim-Kwang Raymond Choo. "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks." *IEEE Internet of Things Journal* 8, no. 12 (2020): 9463-9472. https://doi.org/10.1109/JIOT.2020.2996590

[5] Fatani, Abdulaziz, Mohamed Abd Elaziz, Abdelghani Dahou, Mohammed AA Al-Qaness, and Songfeng Lu. "IoT intrusion detection system using deep learning and enhanced transient search optimization." *IEEE Access* 9 (2021): 123448-123464. https://doi.org/10.1109/ACCESS.2021.3109081

[6] Alhabshy, Abdallah A., Bashar I. Hameed, and Kamal Abdelraouf Eldahshan. "An ameliorated multiattack network anomaly detection in distributed big data system-based enhanced stacking multiple binary classifiers." *IEEE Access* 10 (2022): 52724-52743. https://doi.org/10.1109/ACCESS.2022.3174482

[7] Ravi, Nagarathna, and S. Mercy Shalinie. "Semisupervised-learning-based security to detect and mitigate intrusions in IoT network." *IEEE Internet of Things Journal* 7, no. 11 (2020): 11041-11052. https://doi.org/10.1109/JIOT.2020.2993410

[8] Li, XuKui, Wei Chen, Qianru Zhang, and Lifa Wu. "Building auto-encoder intrusion detection system based on random forest feature selection." *Computers & Security* 95 (2020): 101851. https://doi.org/10.1016/j.cose.2020.101851

[9] KK, P., and B. Retnaswamy. "A Novel MWKF-LSTM Based Intrusion Detection System for the IoT-Cloud Platform with Efficient User Authentication and Data Encryption Models." (2022).

[10] Papamartzivanos, Dimitrios, Félix Gómez Mármol, and Georgios Kambourakis. "Introducing deep learning self-adaptive misuse network intrusion detection systems." *IEEE access* 7 (2019): 13546-13560. https://doi.org/10.1109/ACCESS.2019.2893871

[11] Yang, Yanqing, Kangfeng Zheng, Bin Wu, Yixian Yang, and Xiujuan Wang. "Network intrusion detection based on supervised adversarial variational auto-encoder with regularization." *IEEE access* 8 (2020): 42169-42184. https://doi.org/10.1109/ACCESS.2020.2977007

[12] Liu, Lan, Pengcheng Wang, Jun Lin, and Langzhou Liu. "Intrusion detection of imbalanced network traffic based on machine learning and deep learning." *Ieee Access* 9 (2020): 7550-7563. https://doi.org/10.1109/ACCESS.2020.3048198

[13] Maxime. "What Is a Transformer? - Inside Machine Learning - Medium." Inside Machine learning, January 4, 2019. https://medium.com/inside-machine-learning/what-is-a-transformer-d07dd1fbec04.

[14] Sarhan, Mohanad, Siamak Layeghy, and Marius Portmann. "Feature analysis for machine learning-based IoT intrusion detection." *arXiv preprint arXiv:2108.12732* (2021). https://doi.org/10.21203/rs.3.rs-2035633/v1

[15] Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Łukasz Kaiser, and Illia Polosukhin. "Attention is all you need." *Advances in neural information processing systems* 30 (2017).

[16] El-Yahyaoui, Ahmed, and Mohamed Dafir Ech-Cherif El Kettani. "A New Encryption Scheme to Perform Smart Computations on Encrypted Cloud Big Data." In *Lecture Notes in Real-Time Intelligent Systems*, pp. 313-320. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-319-91337-7_29

[17] Wu, Zihan, Hong Zhang, Penghai Wang, and Zhibo Sun. "RTIDS: A robust transformer-based approach for intrusion detection system." *IEEE Access* 10 (2022): 64375-64387. https://doi.org/10.1109/ACCESS.2022.3182333

[18] Thirimanne, Sharuka Promodya, Lasitha Jayawardana, Lasith Yasakethu, Pushpika Liyanaarachchi, and Chaminda Hewage. "Deep neural network based real-time intrusion detection system." *SN Computer Science* 3, no. 2 (2022): 145. https://doi.org/10.1007/s42979-022-01031-1

[19] Attota, Dinesh Chowdary, Viraaji Mothukuri, Reza M. Parizi, and Seyedamin Pouriyeh. "An ensemble multi-view federated learning intrusion detection for IoT." *IEEE Access* 9 (2021): 117734-117745. https://doi.org/10.1109/ACCESS.2021.3107337

[20] Arshad, Junaid, Muhammad Ajmal Azad, Muhammad Mahmoud Abdeltaif, and Khaled Salah. "An intrusion detection framework for energy constrained IoT devices." *Mechanical Systems and Signal Processing* 136 (2020): 106436. https://doi.org/10.1016/j.ymssp.2019.106436

[21] Mijwil, Maad, Israa Ezzat Salem, and Marwa M. Ismaeel. "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review." *Iraqi Journal For Computer Science and Mathematics* 4, no. 1 (2023): 87-101. https://doi.org/10.52866/ijcsm.2023.01.01.008.

[22] Rammo, Fawziya M., and Mohammed N. Al-Hamdani. "Detecting the speaker language using CNN deep learning algorithm." *Iraqi Journal for Computer Science and Mathematics* 3, no. 1 (2022): 43-52. https://doi.org/10.52866/ijcsm.2022.01.01.005

[23] Satyanarayana, P., G. Diwakar, B. V. Subbayamma, NV Phani Sai Kumar, M. Arun, and S. Gopalakrishnan. "Comparative analysis of new meta-heuristic-variants for privacy preservation in wireless mobile adhoc networks for IoT applications." *Computer Communications* 198 (2023): 262-281. https://doi.org/10.1016/j.comcom.2022.12.006

[24] Satyanarayana, P., Usha Devi Yalavarthi, Yadavalli SS Sriramam, M. Arun, V. Gokula Krishnan, and S. Gopalakrishnan. "Implementation of Enhanced Energy Aware Clustering Based Routing (EEACBR) Algorithm to Improve Network Lifetime in WSN's." In *2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, pp. 1-6. IEEE, 2022. https://doi.org/10.1109/ICMNWC56175.2022.10031991