International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 02, Issue 01, January-February (2024)

RESEARCH ARTICLE

SAFE-ACID: A NOVEL SECURITY ASSESSMENT FRAMEWORK FOR IOT INTRUSION DETECTION VIA DEEP LEARNING

G. Sreetha [1,*] and G. Santhiya [2]

[1] Department of Computer Science and Engineering, Arunachala college of Engineering, Manavilai, India.
[2] Department of Computer Science and Engineering, SRM Valliammai Engineering College,Chennai, India.

Corresponding e-mail: sreethasree2000@gmail.com

Abstract –Internet of Things (IoT) intrusion detection is crucial for ensuring the security of interconnected devices in our digital world. With diverse devices communicating in complex networks, IoT environments face vulnerabilities such as dos attacks and unauthorized access. This paper proposes a novel Security Assessment FramEwork using Attention based Cnn-bigru for Iot Devices (SAFE-ACID) technique that preprocesses data through one-hot encoding, extracts features using Principal Component Analysis, and utilizes an Attention-based CNN-BiGRU model for intrusion detection. The study compares the proposed method with existing techniques using datasets like DS2OS, UNSW-NB15, and ToN_IoT, demonstrating superior presentation in terms of accuracy, F1 score, precision, detection rate, and security rate.According to the comparative analysis, the proposed technique's detection rate is higher than the existing DRF-DBRF, HDA-IDS, and IDS-SIoEL techniques by 16.09%, 4.27%, and 6.9% respectively.

***Keywords** – Deep learning, Internet of Things, Intrusion detection, One-hot encoding.*

1. INTRODUCTION

Internet of Things (IoT) intrusion detection has emerged as a critical aspect of ensuring the security and resilience of interconnected devices in our increasingly digital world [1]. The IoT [2] concept entails the networking of several items, from wearable technology and driverless cars to smart household appliances and industrial gear. These devices build a complicated web of interactions when they communicate with the wider network and one another, which makes them vulnerable to malicious activity [3].

IoT intrusion detection [4] is an essential part of cybersecurity in general because it handles the threats that result from IoT devices' interconnectedness. IoT networks, in contrast to traditional computing systems, comprise a wide range of devices with different functionalities, communication protocols, and security levels. The more IoT devices there are on the market, the greater the potential attack surface for cybercriminals. To quickly detect and address instances of unauthorized access, data breaches, and other security issues, it is critical to have strong intrusion detection systems in place [5].

Deep Learning [6] is important because it can adapt to new threats and learn from them without explicit programming, which is important for IoT intrusion detection. To ensure that deep learning-based intrusion recognition schemes are effective in protecting the integrity and security of IoT ecosystems, it is important to carefully address the complex issues raised by the unique characteristics of IoT environments, such as resource constraints, diverse data types, and dynamic network structures [7,8]. To address these challenges a novel Security Assessment FramEwork using Attention based Cnn-bigru for Iot Devices (SAFE-ACID) technique has been proposed to detect the vulnerabilities in IoT devices. The following is a list of the paper's main contributions.

- Initially, the data from the datasets are pre-processed using one hot encoding to format the data into the suitable format.
- After that, the features are extracted from the pre-processed data using Principal Component Analysis approach to reduce the dimensionality.
- Finally, the extracted features are given to the attention-based CNN-BiGRU model to detect the intrusion in the IoT devices. The output is classified into 2 classes, namely: attack detected and no attack.

The following explanation applies to the remaining portion of this study: Based on the literature, Section II analyses the study. A comprehensive explanation of the suggested system is given in Section III. The outcome and discussion are shown in Section IV, and the conclusion is shown in Section V.

2. LITERATURE SURVEY

In recent years, numerous researches have employed various methodologies to identify vulnerabilities and threats. A number of the contemporary evaluation techniques are discussed in the part that follows, along with some of their drawbacks:

In 2024, Rabie, O.B.J., et al., [9] developed DRF-DBRF security model, combining Descriptive Back Propagated Radial Basis Function classification with Decisive Red Fox optimization to create advanced yet basic security architecture to shield IoT from cyber-attacks.A study of all observed findings shows that the mixture of DRF-DBRF performs better than the other anomaly recognition strategies with improved exactness (99%), correctness (99.2%), f1-score (98.9%), and recall (99%).

In 2024, Li, S., et al., [10] suggested the Hybrid DoS Attack Intrusion Detection System (HDA-IDS), which successfully spots both identified and unidentified DoS/botnet assaults by combining anomaly-based and signature-based recognition. This research also presents CL-GAN, a unique anomaly-based detection approach.The HDA-IDS performs better than other IDSs in identifying botnet and DoS assaults, according to trial results. The HDA-IDS outperformed previous efforts in terms of correctness, F1-Score, recall, and precision,improving performance by an average of 5% overall.

In 2023, Hazman, C., et al., [11] introduced IDS-SIoEL, a revolutionary intrusion detection system with ensemble learning for Internet of Things-based smart settings.Using the GPU, the suggested model was assessed on the Edge-IIoT, BoT-IoT, and IoT-23 datasets. With an almost 99.9% record detection rate and computation durations of 33.68 s for learning and 0.02156 s for detection, our method outperforms the current IDS in terms of ACC, recall, and precision.

In 2023, Elnakib, O., et al., [12] suggested an improved anomaly-based Intrusion Detection Deep Learning Multiclass organization model (EIDM) that uses the CICIDS2017 dataset to categorize 15 traffic behaviors, including 14 different forms of attacks, with a 95% accuracy rate.After measuring the five models' accuracy, it was determined that the suggested model, EIDM, performed better than the other four copies, outperforming them with ancorrectness of 99.48% while also taking time cost into account.

In 2023, Wang, S., et al., [13] suggested an intrusion detection model called Res-TranBiLSTM that reflects the temporal and geographical characteristics of system traffic utilizing ResNet, Transformer, and BiLSTM.The suggested model outperforms the other models, according to the findings, which show accuracy levels of 90.99%, 99.56% and 99.15%, on the CIC-IDS2017 dataset, MQTTset dataset, and, NSL-KDD dataset respectively.Res-TranBiLSTM enhances detection performance for every attack type in addition to improving detection performance overall.

In 2022, Al Razib, M., et al., [14] suggested a Software Defined Networking Enabled Deep Learning-Based Intrusion Detection System (DNNLSTM) to contest developing cyber threats in the IoT. A comprehensive performance matrix is used to assess the effectiveness of the suggested model, taking into account a number of important variables such as recall, F1 score, accuracy, and precision. With previously unheard-of performance implications, such as 99.44% recall, 99.36% precision, 99.42% F1 score, and 99.55% accuracy.

In 2022, Alsulami, A.A., et al., [15] suggested a predictive ML model to identify and categorize system activities in an Internet of Things scheme. Using this method, normal and anomalous network activity can be distinguished. The learning models were assessed against the new and extensive IoTID20 dataset for IoT risks. According to the experimental evaluation, all created models had a detection accuracy of 100% and a classification accuracy ranging from 99.4 to 99.9%.

However, a number of relevant studies have been carried out to find IoT device vulnerabilities. Furthermore, the current approaches have several drawbacks, like reduced accuracy, limited scalability, tighter latency limits, etc. The method to overcome these drawbacks suggested in this article is described in the session that follows.

3. PROPOSED METHOD

In this section, a novel Security Assessment Frame work using Attention based Cnn-bigru for Iot Devices (SAFE-ACID) technique has been proposed to detect vulnerabilities in IoT devices. Initially, the data from the datasets are pre-processed using one hot encoding to format the data into the suitable format. After that, the features are extracted from the pre-processed data using Principal Component Analysis approach to reduce the dimensionality. Finally, the extracted features are given to the attention-based CNN-BiGRU model to detect the intrusion in the IoT devices. The output is classified into 2 classes, namely: attack detected and no attack. The proposed method's whole framework is shown in Figure 1.

3.1. Dataset Description

The proposed design starts with data collection and observation. DS2OS, UNSW-NB15, and ToN_IoT, the three most recent security datasets, are used to train and evaluate the suggested model. Each dataset has a brief description listed below.

3.1.1. DS2OS

The effectiveness of AI-created cyber security plans for smart cities, smart industries, and numerous extra IoT claims may be assessed with this open-source dataset. A total of 357952 samples makes up the DS2OS; of them, 347935 are categorized as normal samples and 10017 as aberrant ethics. There are 8 classes and 13 characteristics in this collection.

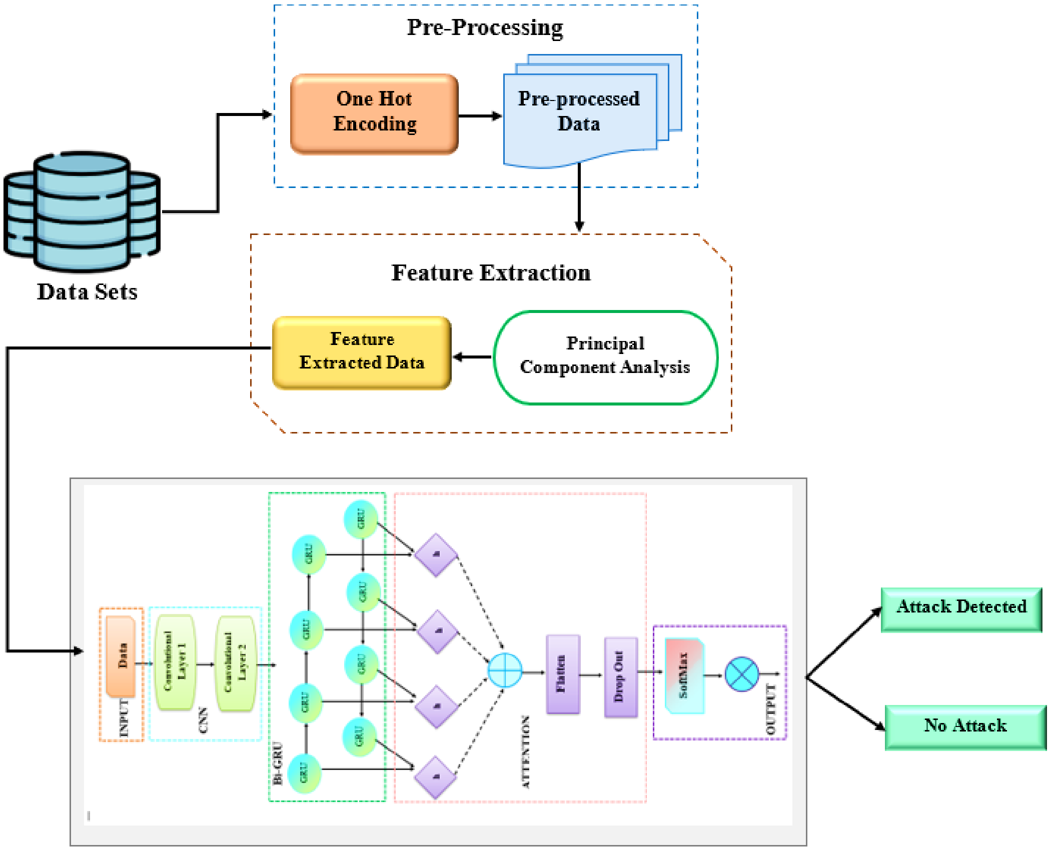

Figure 1. Overall Workflow of the Proposed Method

3.1.2. UNSW-NB15

The Australian Centre for Cyber Security's Cyber Range Lab published this extremely useful dataset in 2015. There are 257673 samples in the UNSW-NB15 total; 93000 of these are categorized as normal samples, while 164673 are malicious samples. Ten classes and forty-nine features make up this dataset.

3.1.3. ToN_IoT

For IoT/IIoT applications, this is one of the most recent datasets. In 2019, the Cyber Range and IoT Labs at the University of New South Wales in Australia gave a presentation about it. This is a helpful dataset for assessing the fidelity and effectiveness of various ML/DL-based cybersecurity systems. There are 1379274 samples in the ToN_IoT, of which 270279 are considered normal samples and 1108995 are aberrant standards. There are ten classes in this dataset.

3.2. Preprocessing

Preprocessing is the grouping of steps and techniques used to adjust unprocessed data prior to additional analysis. The goal of preprocessing is to format data such that it is suitable for the task at hand. The dataset's data were pre-processed for additional processing by converting textual data into numerical data using the one hot encoding approach.

3.2.1. One Hot Encoding

A popular method for capturing strings with a finite number of values is one-hot encoding, which makes use of a sparse vector with one member set to 1 and all other elements set to 0. One-hot encoding is simple and produces a sparse matrix with a large percentage of zeros as values. High cardinality will result in high dimensional feature trajectories when using one-hot encoding. For each category in the categorical variable, it constructs binary columns where a "1" denotes the existence of that category and a "0" denotes its absence. Let D be a categorical variable with cardinality $l \geq 2$ such that $dom(D) = \{b_n, 1 < n \leq l\}$ and $g^j(D) = b^j$. Each feature vector is encoded once using the one hot approach as follows:

$$Z^j = [1_{\{b_1\}}(b^j), 1_{\{b_2\}}(b^j), \dots \dots . . 1_{\{b_l\}}(b^j)] \in \mathbb{R}^l \qquad (1)$$

Where $1_{\{b_1\}}(.)$ is an indicator function over the singleton b_m. One-hot encoding is designed to be utilized in situations when categories are mutually exclusive, which is not always the case with dirty data. One-hot encoding prevents unintentional biases by using binary columns to verify that distances across categories are equal. Using this method, the data is converted from string information to numerical data.

3.3. Feature Extraction

One of the most important phases in the preparation of data for deep learning models is feature extraction. To enhance the model's performance, the most pertinent information from the raw data must be chosen or transformed. The preprocessed data is subjected to feature extraction using the Principal Component Analysis method.

3.3.1. Principal Component Analysis (PCA)

A popular method for reducing feature dimensionality is PCA. Conventional PCA reduces the dimensions linearly; hence it is ineffective when the feature space is complex. Standard PCA is generalized to nonlinear dimension reduction to improve the feature reduction process. After the features have been normalized, PCA is a helpful feature dimension reduction technique. Dimensionality reduction techniques such as PCA are used to identify the eigenvectors of the covariance matrix with the largest eigenvalues, hence lowering the dimensionality of large datasets.PCA algebraic definition is as follows, Calculate the mean of A for data framework A as follows:

$$\delta = F(A) \tag{2}$$

Determine A's covariance as follows:

$$CU = C_{ov}(A) = F[(A-\delta)(A-\delta)^T \tag{3}$$

Count the eigenvalue δ_i, and eigenvector b_1, b_2,……...b_N, j= 1, 2……N of the covariance CoV. The equation is solved for the Covariance CoV;

$$V_k = \frac{\sum_{i=1}^{L}\delta_n}{\sum_{i=1}^{M}\delta_n} \tag{4}$$

The mutual range should be 83% greater than the size of the major segments, therefore choose the first L eigenvalue that did this, information about a more compact measurement subspace,

$$g = V^t - X \tag{5}$$

Where X is the original data that was knotted, and t denotes the transfer matrix. Operating the main L eigenvector independently from n to $K(K \ll n)$.) increases the number of variables or measurements.

$$|\delta l - C0V| = 0 \tag{6}$$

Whereas,l give the identity matrix credit for having dimensions that resembles CoV. Decide on the δ_n Eigenvalues of the component L by counting the proportion of the data that the first component accounts. The removed features are given to the detection module to find the intrusion.

3.4. Attention based CNN-BiGRU

The construction of the attention-based CNN-BiGRU is exposed in Figure 2. The input layer, CNN layer, BiGRU layer, Attention layer, and output layer comprise the model.An attention-based CNN-BiGRU archetypal for intrusion recognition is designed to effectively capture spatial patterns with convolutional layers (CNN), temporal dependencies with bidirectional gated recurrent units (BiGRU), and prioritize relevant information using an attention mechanism. This architecture aims to distinguish between normal network behavior and potential attacks, classifying the output into two classes: Attack Detected and No Attack.

The CNN layer uses two convolutional layers to apply feature execution on the input sensor data. We use convolutional kernels with lengths of 5 and 3 to extract deep feature maps of different sizes. Each CNN layer contains 64 ReLU activation functions and 64 convolution kernels to extract 64 feature maps. Two convolutional layers are sufficient to fully extract the hierarchical abstract properties of acceleration data. The output of the CNN must be a feature map which is given in equation (7).

$$Y = a(v_a * X + bs) \tag{7}$$

Here, the generated feature map is represented as Y, and the weight of the trainable filter is v_a, the input data is represented as X, the bias term is bs and the activation is denoted as a. The CNN retrieved high-level features are sent into the BiGRU layer, along with 32 hidden units. GRU equations are used to compute the forward hidden state and the backward hidden state are shown in equation (8) and (9).

$$H^{fw} = GRU_{fw}(w_l, H_{l-1}^{fw}) \tag{8}$$

$$H^{bw} = GRU_{bw}(w_l, H_{l+1}^{bw}) \tag{9}$$

Here, H^{fw} indicates the forward hidden state and H^{bw} represents the backward hidden state. Based on the concatenated hidden states from the BiGRU layer, the attention mechanism calculates attention weights w_l for each time step which is shown in equation (10)

$$w_l = tanh(Wi_w \cdot [H^{fw}, H^{bw}] \tag{10}$$

Where, Wi_w represents the attention weight matrix. A weighted sum of the BiGRU hidden states is used to calculate the context vector V_l for each time step which is shown in equation (11)

$$V_l = \sum_{j=1}^{L} a_j\, [H^{fw}, H^{bw}] \tag{11}$$

To create a one-dimensional feature map, the resulting feature matrix is imported into the flattening layer for feature fusion, and the dropout layer is added after the flattening layer to prevent over fitting.The feature matrix produced by the attention layer is the input of the output layer, which uses the classifier SoftMax to classify the intrusion detection. The result can be determined as

$$Z_t = softmax(W_z \cdot Cn_t, +b_z) \tag{12}$$

where W_z and b_z represent the output layer's weight matrix and bias vector respectively. Finally, the output is classified into two classes they are attack detected and no attack in IoT devices.

4. RESULT AND DISCUSSION

In this section, the new discoveries of the proposed SAFE-ACID method are analysed and performance is discussed in terms of multiple assessment metrics. The Python programming language and libraries are used in the development and evaluation of the suggested framework. The proposed model’s effectiveness is contrasted with DRF-DBRF [9], HDA-IDS [10], and IDS-SIoEL [11] in terms ofF1-Score, accuracy, detection rate, precision, and security rate.

4.1. Performance Analysis

In this section, the accuracy, exactness, and recall of the proposed SAFE-ACID method have been compared to those of existing techniques, including DRF-DBRF [9], HDA-IDS [10], and IDS-SIoEL [11].

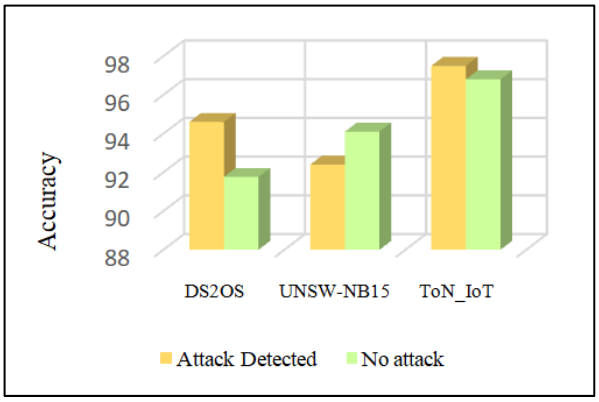

Figure 2. Performance Comparison in terms of Accuracy

The accuracy of detecting attack and no attack using the DS2OS, UNSW-NB15 and ToN_IoT datasets is exposed in Figure 3. It validates that applying the proposed SAFE-ACID technique to the ToN_IoT dataset results in a greater accuracy rate in attack detected. Additionally, employing the suggested technique with the ToN_IoT dataset results in a greater accuracy rate in the no attack.

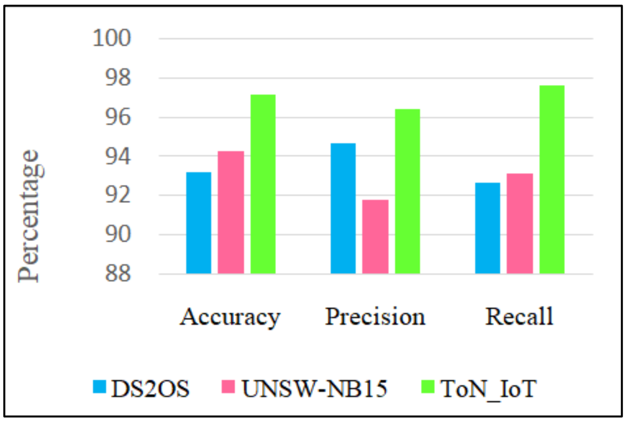

Figure 3. Overall Performance Comparison

Figure 3. Illustrates the Performance comparison of accuracy, precision, F1 score using three data sets they are DS2OS, ToN_IoT, andUNSW-NB15. The outcomes show that the model beats using DS2OSdataset with accuracy, and precision, F1 scores are 93.18%, 94.7% and 92.67% respectively.Using UNSW-NB 15 dataset the model outperforms 94.25%, 921.8%, and 83.1% for accuracy, precision, F1 score respectively. Using ToN_IoT dataset the model outperforms 97.15%, 96.41%, and 97.67% for accuracy, precision, F1 score respectively.

4.2. Comparative Analysis

This section includes simulations to evaluate the effectiveness of the proposed SAFE-ACID technique. DRF-DBRF [9], HDA-IDS [10], and IDS-SIoEL [11] techniques are contrasted with the proposed technique. The proposed SAFE-ACID approach is evaluated using a factor, including accuracy, precision, F1-Score, detection rate, and security rate.

In Fig. 4, the proposed SAFE-ACID technique, and the existing method such as DRF-DBRF [9], HDA-IDS [10], and IDS-SIoEL [11] are contrasted for the accuracy via the UNSW-NB 15 DS2OS,and ToN_IoT datasets. The accuracy of the proposed SAFE-ACID system for detecting attacks is increased by 15.1%, 5.85%, and 8.94% as compared to the existing method using DS2OS dataset and increases by 26.1%, 9.59%, and 8.38% using UNSW-NB 15 dataset and increases by 12.9%, 7.06%, and 6.45% using ToN_IoT dataset respectively.

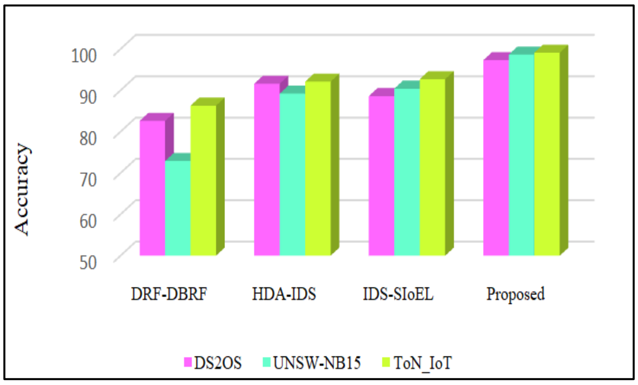

Figure 4. Overall Accuracy Comparison

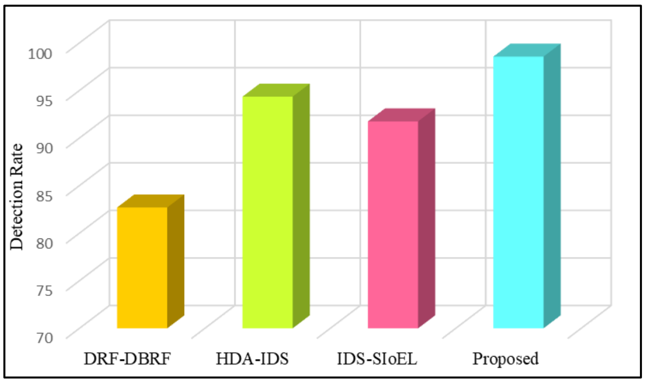

Figure 5. Detection Rate Comparison

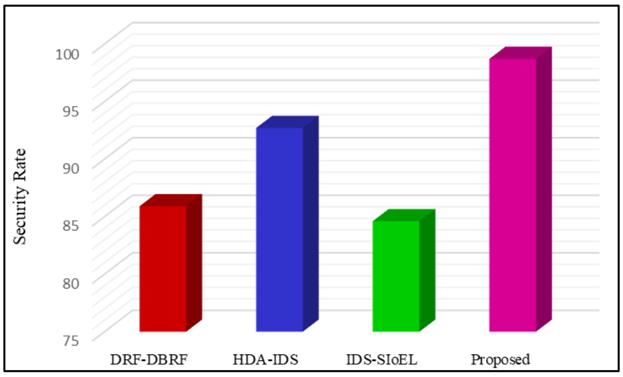

Figure 6. Comparison in terms of security rate

The above Fig 5. describes the presentation comparison of the detection rate for the proposed SAFE-ACID technique and the current techniques such as DRF-DBRF [9], HDA-IDS [10], and IDS-SIoEL [11] using the datasets. The proposed SAFE-ACID technique has a higher detection rate compared to the other existing system. The detection rate is 16.09%, 4.27%, and 6.9% higher than the existing method such as DRF-DBRF, HDA-IDS, and IDS-SIoEL respectively.

The efficiency of each strategy in defending systems is displayed in Figure 6, which compares security rates between suggested SAFE-ACID technique and current intrusion detection techniques. This graphic study highlights the importance of staying up to date with cutting-edge techniques to improve overall security against evolving cyberthreats and raises awareness of potential developments in intrusion detection technology.

5. CONCLUSION

In this paper, a novel Security Assessment Frame work using Attention based Cnn-bigru for Iot Devices (SAFE-ACID) technique has been proposed to detect vulnerabilities in IoT devices. The vulnerability is detected by using attention-based CNN-BiGRU Model which classifies the output into 2 classes as attack detected and no attack. The proposed framework is developed and assessed using the Python. The efficiency of the proposed technique has been determined via assessment metrics such as recall, accuracy, security rate, precision, detection rate, and F1 score. According to the comparative analysis, the proposed technique's detection rate is higher than the existing DRF-DBRF, HDA-IDS, and IDS-SIoEL techniques by 16.09%, 4.27%, and 6.9% respectively. Numerous industries have shown that block chain technology has the ability to increase security and transparency. Potential research topics include the feasibility of integrating block chain technology with IoT security assessment.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] L. Kasowaki, and K. Ali, *Cyber Hygiene: Safeguarding Your Data in a Connected World*, no. 11698, 2024. [Cross Ref] [Google Scholar] [Publisher Link]

[2] M. Amanullakhan, M. Usha and S. Ramesh, "Intrusion Detection Architecture (IDA) In IOT Based Security System", *International Journal of Computer and Engineering Optimization*, Vol. 01, no. 01, pp. 33-42, 2023. [Cross Ref] [Google Scholar] [Publisher Link]

[3] A.K. Tyagi, "Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications", *In AI and Blockchain Applications in Industrial Robotics*, pp. 171-199, 2024. [Cross Ref] [Google Scholar] [Publisher Link]

[4] M. Amanullakhan, M. Usha and S. Ramesh, "Intrusion Detection Architecture (IDA) In IOT Based Security System", *International Journal of Computer and Engineering Optimization*, Vol. 01, no. 01, pp. 33-42, 2023. [Cross Ref] [Google Scholar] [Publisher Link]

[5] D. Everson, and L. Cheng, "A Survey on Network Attack Surface Mapping", *Digital Threats: Research and Practice*, 2024. [Cross Ref] [Google Scholar] [Publisher Link]

[6] M. Prabhu, G. Revathy and R. Raja Kumar, "Deep Learning Based Authentication Secure Data Storing in Cloud Computing", *International Journal of Computer and Engineering Optimization*, Vol. 01, no. 01, pp. 10-14, 2023. [Cross Ref] [Google Scholar] [Publisher Link]

[7] M. Karthikeyan, D. Manimegalai, and K. RajaGopal, "Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection", *Scientific Reports*, vol. 14, no. 1, pp.231, 2024. [Cross Ref] [Google Scholar] [Publisher Link]

[8] P. Potnurwar, I"ntrusion Detection System for Big Data Environment Using Deep Learning". 2024. [Cross Ref] [Google Scholar] [Publisher Link]

[9] O.B.J. Rabie, S. Selvarajan, T. Hasanin, A.M. Alshareef, C.K. Yogesh, and M. Uddin, "A novel IoT intrusion detection framework using Decisive Red Fox optimization and descriptive back propagated radial basis function models", *Scientific Reports*, vol. 14, no. 1, pp.386, 2024. [Cross Ref] [Google Scholar] [Publisher Link]

[10] S. Li, Y. Cao, S. Liu, Y. Lai, Y. Zhu, and N. Ahmad, "HDA-IDS: A Hybrid DoS Attacks Intrusion Detection System for IoT by using semi-supervised CL-GAN", *Expert Systems with Applications*, vol. 238, pp.122198, 2024. [Cross Ref] [Google Scholar] [Publisher Link]

[11] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning",*Cluster Computing*, vol. 26, no. 6, pp.4069-4083, 2023. [Cross Ref] [Google Scholar] [Publisher Link]

[12] O. Elnakib, E. Shaaban, M. Mahmoud, and K. Emara, "EIDM: deep learning model for IoT intrusion detection systems",*The Journal of Supercomputing*, pp.1-21, 2023. [Cross Ref] [Google Scholar] [Publisher Link]

[13] S. Wang, W. Xu, and Y. Liu, "Res-TranBiLSTM: An intelligent approach for intrusion detection in the Internet of Things", *Computer Networks*, vol. 235, pp.109982, 2023. [Cross Ref] [Google Scholar] [Publisher Link]

[14] M. Al Razib, D. Javeed, M.T. Khan, R. Alkanhel, and M.S.A. Muthanna, "Cyber threats detection in smart environments using SDN-enabled DNN-LSTM hybrid framework", *IEEE Access*, vol. 10, pp.53015-53026, 2022. [Cross Ref] [Google Scholar] [Publisher Link]

[15] A.A. Alsulami, Q. Abu Al-Haija, A. Tayeb, and A. Alqahtani, "An Intrusion Detection and Classification System for IoT Traffic with Improved Data Engineering", *Applied Sciences*, vol. 12, no. 23, pp.12336, 2022. [Cross Ref] [Google Scholar] [Publisher Link]

AUTHORS

G. Sreetha, she was born in Kanyakumari District, Tamilnadu, India in 2000. She received her BE degree in computer science and engineering from Arunachala college of engineering, Manavilai, Anna University, India in 2021. Currently she is completed her ME degree in computer science and engineering from Arunachala college of Engineering, Manavilai, Anna University, India in 2023. Her interested research area is cloud computing, IoT, Deep learning and cryptography.

G. Santhiya received the B.E. degree in Computer Science and Engineering from Anna University, Chennai, India, in 2010 M.E degree in Software Engineering from Noorul Islam Centre for Higher Education, Kumaracoil, India in 2012. She is currently pursuing the Ph.D. degree with Anna University, Chennai, India. Currently, she is working as an Assistant Professor at SRM Valliammai Engineering College, Kattankulathur, Chennai with the Department of Information Technology, Anna University, Chennai, India. Her current research interests include machine learning, the Internet of Things (IoTs), and sensor networks.

Arrived: 20.12.2023

Accepted: 21.02.2024