

Gated dilated causal convolution-based encoder-decoder network for IoT intrusion detection

Aarthi Gopalakrishnan, Sharon Priya Surendran, Aisha Banu Wahab

Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India

Article Info

Article history:

Received Apr 12, 2024

Revised Mar 14, 2025

Accepted Jun 23, 2025

Keywords:

BoT-IoT dataset

Deep learning

GDCC-ED

Internet of things

Intrusion detection

ABSTRACT

The internet of things (IoT) is perhaps the greatest modern development, as it affects our daily lives and is rapidly expanding in its application zones. The IoT is used in everyday activities, so security is more crucial because intrusion detection will introduce and eliminate attacks. In this paper, a novel deep learning based intrusion detection technique (DEBIT) has been proposed that detects the intrusion using deep learning techniques efficiently. Initially, the data from IoT user is preprocessed and classified using the novel gated dilated casual convolution based encoder-decoder (GDCC-ED) method, which classifies the data into attack and non-attack. The proposed DEBIT framework has been assessed using a MATLAB simulator. The performance of the proposed DEBIT framework has been assessed based on specific parameters, including recall, detection rate, accuracy, F1 score, and precision. Based on experimental results, the suggested method is 99.5% more accurate than pigeon-inspired optimization (PIO), Res-TranBiLSTM, and blockchain-based African buffalo (BbAB), which are 85.4%, 92.5%, and 85%, respectively.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Sharon Priya Surendran

Department of Computer Science and Engineering

B.S. Abdur Rahman Crescent Institute of Science and Technology

Chennai, India

Email: sharonpriya@crescent.education

1. INTRODUCTION

The internet of things (IoT) is a relatively recent invention transform the way people live, work, and enjoy life [1]. In industries like manufacturing, health, agriculture, education, and tourism, this technology gives businesses and organizations enormous business value [2], [3]. IoT is a new paradigm for communication like uses sensors to let objects detect their surroundings, talk to another, and transfer data on the internet [4], [5].

In the years that follow, there will be an unprecedented amount of IoT devices associated to the internet [6], [7]. The availability, integrity, and data privacy are seriously endangered by its growing volume, and malicious actors may exploit all of these aspects [8]. IoT security has gained more attention as a result of a number of innovative apps that make use of connected devices that have been developed recently [9, 10].

Considering the security measures, it is vital to build a security model for an IoT environment [11]. To prevent harmful users from gaining unwanted access to data sources, data-oriented security measures must be prioritized. Many artificial intelligence (AI) approaches, including convolutional neural networks (CNN), support vector machines (SVM), Bayesian networks, and deep belief networks (DBN), are widely used to identify patterns of unusual behavior in IoT networks [12]-[15]. AI is a useful tool that can be used to detect harmful assaults in a timely manner. Even though intrusion detection for IoT networks utilizes a lot of DL techniques, security remains an issue [16], [17].

These studies demonstrate several strategies for enhancing IoT security using efficient intrusion detection systems (IDS) solutions that make utilize of DL, cloud computing, and specialized algorithms [18]. IoT platforms pose a number of challenges, including computational overhead, the complexity of integrating with diverse platforms, managing false positives and false negatives, the inherent cybersecurity risks, the optimization of IDS for resource-constrained environments, the variability of dataset quality, and the emergence of cyber threats within IoT ecosystems [19]. To overcome these challenges several studies like encoder-decoder [20] techniques has been used, yet have posed some challenges [21].

In 2020, Rani and Kaushal [22] suggested a supervised ML technique-based, uniform IDS that is both efficient and uses a Random Forest classifier. The limited storage capacity and computational limits of IoT have led to enhance in the popularity of cloud-based IoT. In 2020, Sicato *et al.* [23] proposed distributed cloud framework with software-defined IDS, which provides a safe IoT environment. An efficient IDS is essential, as evidenced by the rise in both the quantity and range of security threats to these systems. In 2021, Ullah and Mahmoud [24] suggested CNN model is tested using the ID datasets from IoT-23, BoT-IoT, and IoT network intrusion. The classes sparta, normal, and scan are correctly identified. The single misclassification resulted in an FNR of 1.48% for the MQTT brute force assault class.

In 2021, Kalnoor and Gowrishankar [25] provided a high level of security for IoT smart environments by utilizing the innovative intelligent IDS technique. When compared to alternative algorithms, the suggested model's accuracy has been 100%. In 2023, Subramani and Selvi [26] proposed an intelligent IDS to find intrusions in IoT based WSN. By minimizing false positive rates and improving detection accuracy, the studies conducted with CIDD and KDD'99 Cup datasets for evaluation show that the IDS can catch the intruders more precisely. In 2023, Alghanam *et al.* [27] proposed to enhance pigeon-inspired optimization (PIO) by incorporating a local search (LS-PIO) technique. The recommended approach outperforms alternative NIDS methods selected from the literature based on the most recent relevant research, as per the results.

In 2023, Cao *et al.* [28] suggested an ensemble learning process on stacking to create a successful IDS. The experiment's results suggest that proposed IDS may improve IoT device security and reach a huge accuracy rate of 99.68%, which would eventually benefit the users who rely on these devices. In 2023, Wang *et al.* [29] proposed Res-TranBiLSTM, an ID model that considers temporal and geographical characteristics of network traffic. The results demonstrate that recommended system performs better than other systems. In 2023, Saravanan *et al.* [30] proposed to identify intrusions and enhance security by utilizing the African buffalo (BbAB) system. Better high recall of 99.92% and accuracy of 99.87% are achieved by the developed method's performance.

To overcome these issue, offers a DEBIT framework for preventing network attacks on the IoT to detect intrusions. The following are the contributions of the suggested DEBIT framework:

- Initially, the data is collected from the IoT user traffic and this data is fed into preprocessed techniques such as data cleaning, tokenization, lemmatization, and stemming.
- The GDCCB-ED approach is used to process the data and forecast whether an attack or non-attack has occurred.
- The main advantage of the proposed method significantly enhances accuracy in fault prediction by efficiently capturing long-range dependencies and processing temporal data in real time.
- Evaluations of the suggested DEBIT framework's performance have been conducted using particular metrics, including F1 score, detection rate, precision, accuracy, and recall.

The rest of the analysis is arranged as follows: In section 2, finding the literature review on DL techniques for IDS are displayed. Section 3 presents an explanation of the suggested DEBIT methodology. The experimental results are given in section 4, and a study summary is provided in section 5.

2. PROPOSED METHODOLOGY

To overcome the novel proposed in this section, Figure 1 represents the IoT utilizing the DL based intrusion detection (DEBIT) framework. The preprocessing of the proposed framework includes data cleaning, tokenization, lemmatization, and stemming. The GDCCB-ED model is used to process the data and forecast whether an attack or non-attack has occurred. This will be obvious in the final product's quality, which will use an ideal subset of features and increase the possibility of ID in an IoT environment. A thorough explanation of the framework will be provided in the parts that follow.

2.1. Data collection

Several datasets have been used by researchers to assess systems. The UNSW in Canberra produced the BoT-IoT dataset was created for this purpose the UNSW Laboratory. Combining regular traffic with botnets, the environment was formed. Comma separated values (CSV) files and the original file with a cap extension were two of the forms in which the data sources were supplied.

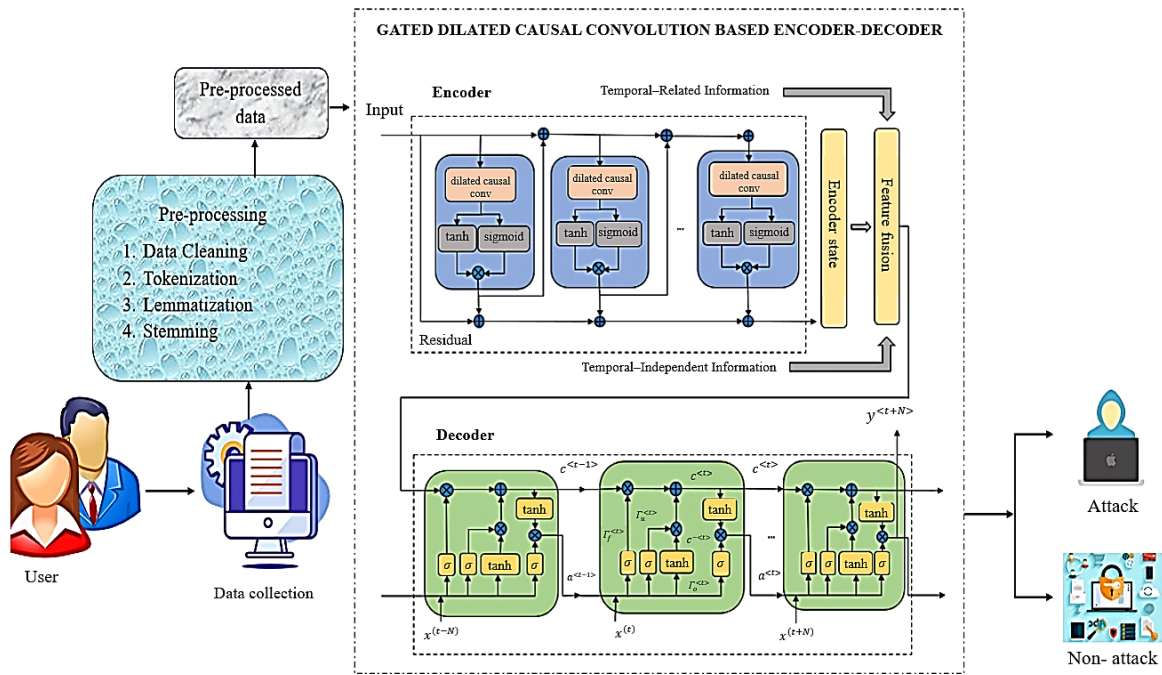


Figure 1. The overall block diagram for the proposed DEBIT framework which contains pre-processing and GDCCB-ED model for intrusion detection

2.2. Pre-processing

Data processing is done in advance to get it ready for main processing or additional analysis. The preprocessing data has split into data cleaning, tokenization, lemmatization, and stemming. The dataset is initially cleaned in this step-in order to get rid of duplicate records. Nevertheless, we make use of the pre-cleaned Bot-IoT dataset. Thus, this cleaning step is not important in our experiment; nevertheless, it is necessary if the original dataset, such as KDD'99, is employed. After data cleaning, the sentence's "tokens," or words and punctuation, appear first. In the textbox below, the output inserts pipe characters in between the tokens. Every inflection is mapped by a lemmatizer to a canonical form called the lemma, which is usually the form found in dictionaries written in the language of the intended audience. We use the Tree Tagger lemmatizer in this study. Text stemming alters words to produce alternative word forms using a variety of linguistic operations, including affixation. For example, "study" is the root of the word "studying".

2.3. Attack detection using GDCC-ED

Encoder-decoder architecture is used in our suggested GDCC-ED model, as seen in Figure 2. Two primary components make up GDCC-ED: i) an encoder that uses a GDCC designed to model long-range temporal dependencies and ii) a decoder for multi-phase network traffic prediction. The proposed framework combines characteristics such as web-based attacks and network harm in addition to the encoder's output.

2.3.1. Encoder for modelling attacks

Three characteristics distinguish the suggested encoder from the standard CNN or RNN. It makes use of three different techniques, which are explained in the sections that follow: i) dilated causal convolutions, ii) gated activations, and iii) residual connections. These techniques help improve learning, capture long-term patterns, and maintain training stability.

- Causal convolution

Raw audio waves are generated by the deep generative model WaveNet. It is where causal convolution first appeared. However, web-based attacks represent serious risks to Industry 5.0 infrastructure when we use them, possibly resulting in the loss of confidential data. In order to reliably detect network harms as soon as they are possible, it is necessary to automatically extract features using conventional approaches.

- Dilated convolutions

The attack surface is increased when IoT devices, big data, and cloud computing are combined, making these systems more at risk for cyberattacks. A network flow happens when two endpoints,

such as a client and a web server, exchange packets back and forth over a set period of time. In our work, a system flow is defined as a series of L ordered collections, where L is the total length of a flow. A flow is denoted as (1).

$$V_L = \{X_1, X_2, \dots, X_L\} \forall M_i \in \mathbb{R}^w \wedge 1 \leq i \leq L \quad (1)$$

Where w is the length of a packet. Describes the distance between variables in a cereal, the absorption value is the most recent parameter to be produced by extended transformations. The dilated causal convolution [20] is depicted in Figure 3.

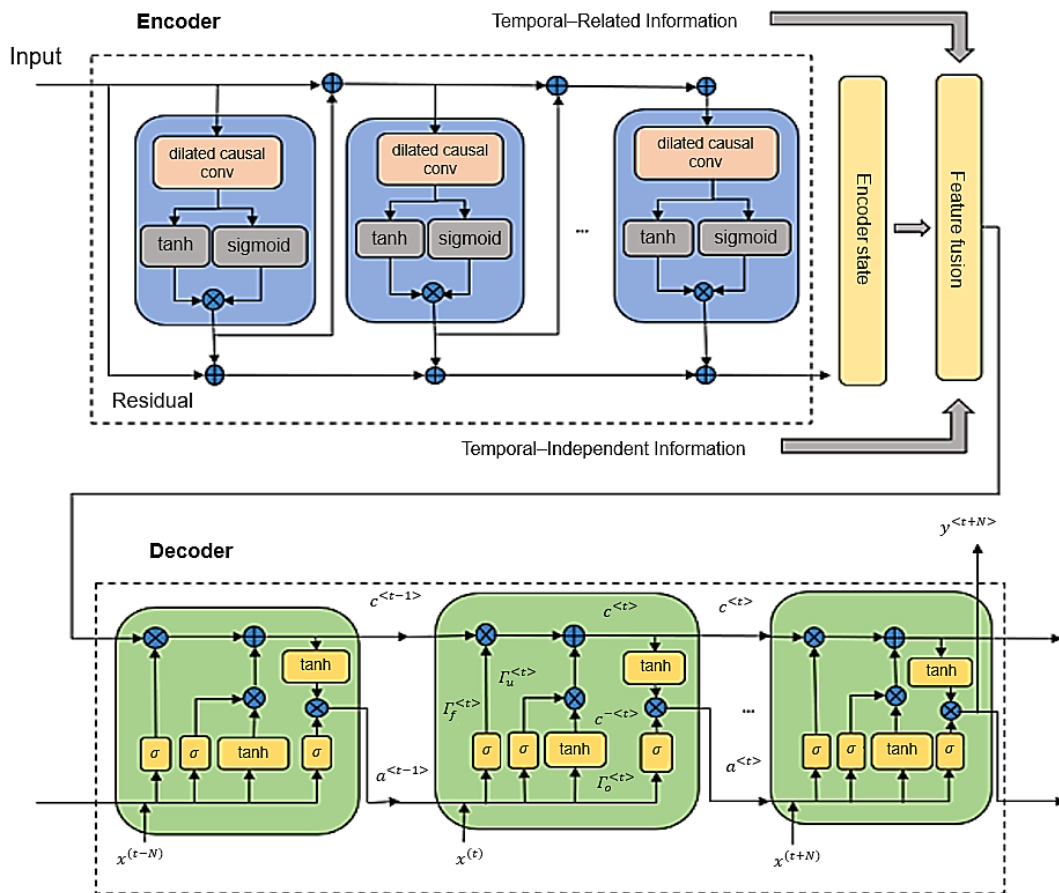


Figure 2. The architecture diagram of the gated dilated causal convolution based encoder-decoder model's which classifies the data into attack or non-attack

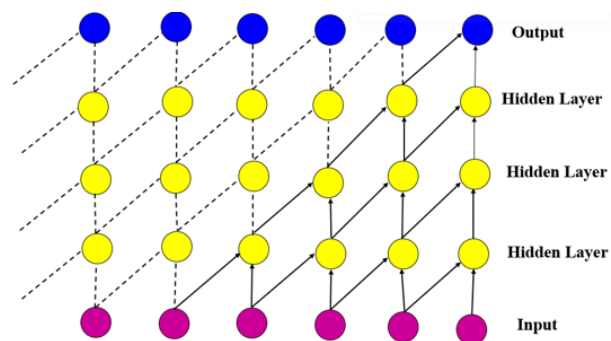


Figure 3. The block diagram of the dilated causal convolution with three hidden layers showing the flow of information from input to output

The following is the formal definition of the extended transformation between the foretell and cereal. This relationship is mathematically expressed in (2).

$$R(n) = (k * \iota r) n = \sum_{\tau=0}^{s-1} k\tau \cdot rn - l\tau \quad (2)$$

Where l is the absorption value and s is the filter size. More particularly, at $l = 1$, extended transformation simplifies to a typical convolution.

- Gated activation

Sigmoid functions are frequently employed as initiation functions, but in this case, it acts as the gating function rather than the initiation function. We have selected the sigmoid function as an attenuation factor for the initiation of the extended transformation since its value range is between 0 and 1. The advantage is being able to more precisely regulate the flow of knowledge via each buried layer. When taken as a whole, these roles are called gated activation. Hence, two components make up the learnable convolution filter: W are divided into W_v for gate and W_h for filter.

- Residual connection

The input and output of two layers are connected via residual connections. Gated activation [20] is shown in Figure 4. The residual function makes use of the distinction between a visualization that is applied to (3).

$$H(c) = F(c) - c \quad (3)$$

The original visualizing $F(c)$ is more difficult to improve than the residual function $H(c)$. As a consequence, the original purpose becomes (4).

$$o = \sigma(c + H(c)) \quad (4)$$

Where the activation function is represented by σ . The addition of remaining connections follows each GDCC-ED from input to convolution to output.

- Decoder for multi-step traffic forecast

The decoder generates the next state by following a series of sequential steps. It processes the current input along with the previous state to predict the next output. This output is then used to update the state for the following time step.

$$\Gamma_f^{<d>} = \sigma(Wv[a^{<d-1>}, x^{<d>}] + b_v) \quad (5)$$

$$\Gamma_u^{<d>} = \sigma(Wn[a^{<d-1>}, x^{<d>}] + b_n) \quad (6)$$

$$c^{<d>} = \tanh(W_x[a^{<d-1>}, x^{<d>}] + b_x) \quad (7)$$

Where $\Gamma_f^{<d>}$, $\Gamma_u^{<d>}$, and $c^{<d>}$ indicate the output gate, hidden state, and candidate for cell state, in that order. The sigmoid function is represented by σ , the hyperbolic tangent function by \tanh , and division-sage combining by o . The (5) defines the size that control the neglect gate's behavior.

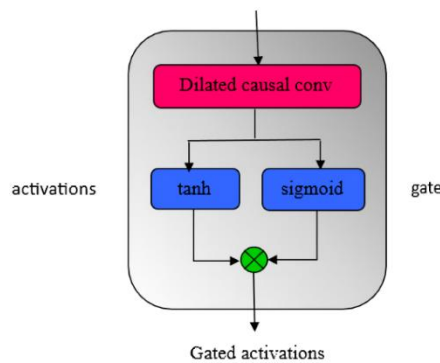


Figure 4. The gated activation mechanism with dilated causal convolution, combining tanh and sigmoid activations for gating

3. RESULTS AND DISCUSSION

The proposed DEBIT method and experimental results are analyzed, and a discussion of efficiency is presented. Using MATLAB stimulation and a Windows OS with an Intel Core i7 CPU and 16GB RAM, the DEBIT framework is constructed and evaluated. The Bot-IoT dataset is utilized to examine the efficacy of the suggested system. The Bot-IoT dataset can be augmented which improves the diversity and robustness of the dataset, thereby enhancing the effectiveness of the suggested DEBIT framework for IoT intrusion detection. The efficacy of the suggested framework is evaluated to the following parameters: F1-score, ROC curve, accuracy, recall, and precision.

3.1. Performance evaluation

In Figure 5, testing and training are conducted. This is to avoid making many attribute calls because these processes are already interdependent. The fact that the training and testing accuracy rose suggests that the convolutional neural network's parameters were truly being appropriately tuned. The testing accuracy was approximately 0 at the beginning and increased to 1 by the thirteenth epoch. Testing loss per batch is still declining at the conclusion of the eleventh epoch, which is consistent with the condition shown by the loss plots.

For attack and non-attack scenarios, Figure 6 displays the F1 scores, recall, accuracy, and precision. Here we find the performance ratio, and the non-attack 95.8% and attack 97.8% will occur. The attack is in the higher accuracy of the graph. The performance ratio for accuracy is 98%. Packet rates for various attacks over specific time intervals. Figure 7 illustrates how to use the black curves to clearly visualize the network traffic patterns, which vary depending on the packet type. Network- and web-based attacks stand out in particular due to the volume of packets they send and cause. Figure 8 displays the ROC curve obtained from the suggested IDS assessed with the BoT-IoT dataset. In this case, the y-axis represents the true positive rate, and the x-axis illustrates the false positive rate. Two classes are represented by the ROC curve.

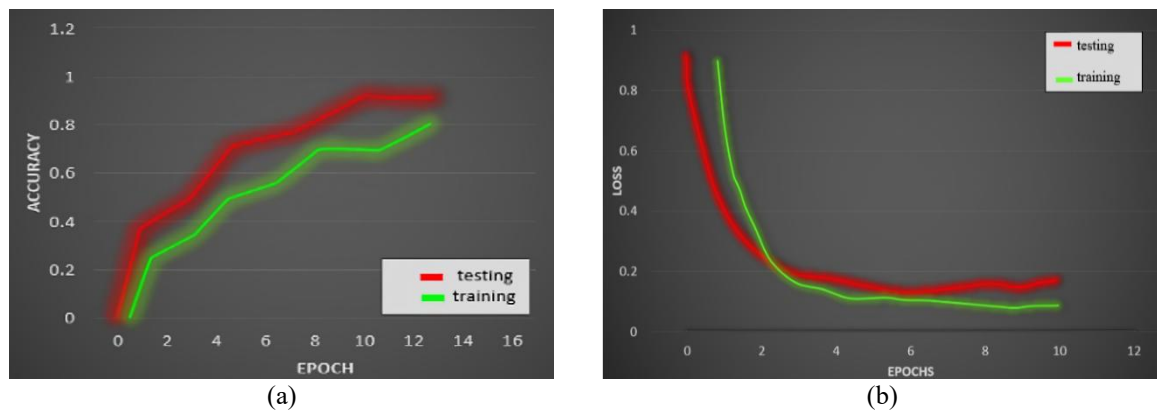


Figure 5. The testing and training using the Bot-IoT dataset: (a) the accuracy and (b) the loss graph

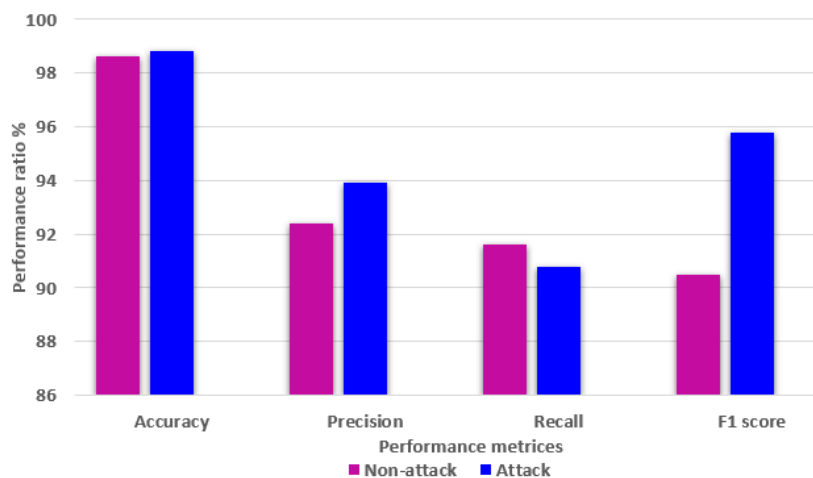


Figure 6. The efficiency ratio of the suggested DEBIT approach for attack and non-attack scenarios

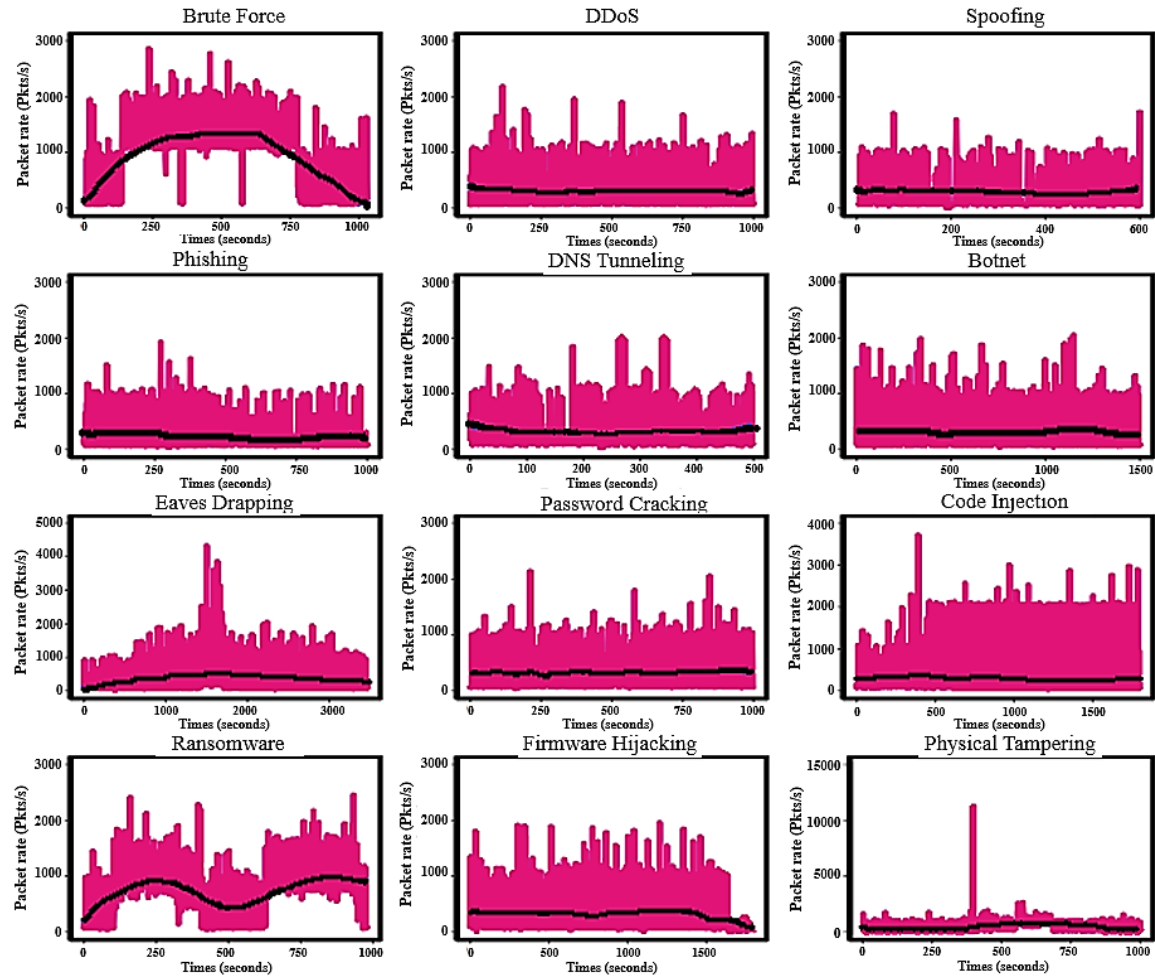


Figure 7. The quantitative pattern of network packet attacks for various attacks over specific time intervals

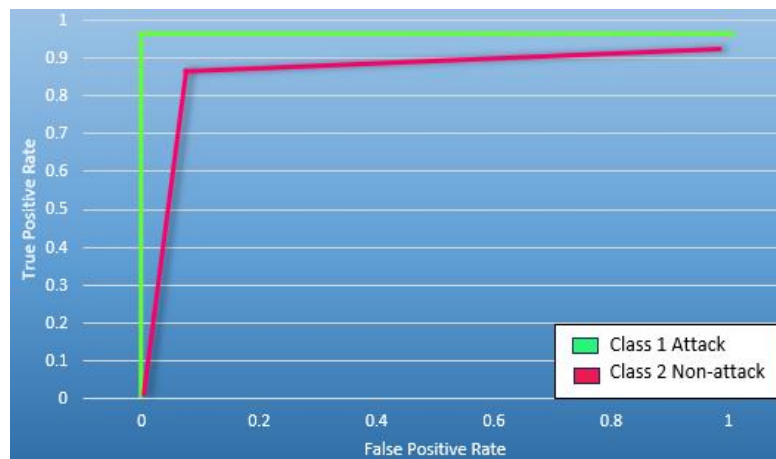


Figure 8. The ROC curve obtained from the suggested IDS assessed with the BoT-IoT dataset

3.2. Comparison analysis

The trade-off between ADR and FAR is represented by a detection rate graph, displayed in Figure 9. With the same dataset, the detection rate may also be used to compare multiple IDSs. IDS performance over time can also be evaluated. The time performance is the overall time required by the IDS to identify an intrusion. The propagation time and the processing time compose this amount of time. In order to process intrusions in real time, the intrusion detection system's processing speed needs to be as fast as possible.

In Figure 10, PC graph's x-axis shows recall, F1 scores, accuracy, and precision, while the y-axis reflects PIO, Res-TranBiLSTM, BbAB, and DEBIT. The results show that for F1-score measurement, the PIO reached 82.6%, the Res-TranBiLSTM reached 80.4%, the BbAB reached 71.6%, and the DEBIT reached 88.4%. For accuracy, the performance with a score of PIO reached 85.4%, the Res-TranBiLSTM reached 92.5%, the BbAB reached 85%, and the DEBIT reached 99.5%. Based on these results, the deep learning techniques are all calculated based on performance comparisons. Table 1 depicts the trends of the runtime of the suggested with existing architectures in different epochs. According to this table, the proposed architecture has achieved the shortest runtime.

Figure 11 shows the scalability efficacy is compared with the other existing approaches. This suggests that the DEBIT approach efficiently handles increasing amounts of data without a significant drop in performance, which is a key advantage when dealing with larger datasets. The consistent performance across all transaction sizes shows that the DEBIT model is reliable and robust for handling varying data loads, unlike the other models, which show fluctuations and instability in scalability.

The proposed method is designed for practical implementation in clinical settings to enhance the accuracy of medical diagnoses through automated image and data classification. By integrating this system into healthcare facilities, medical professionals can leverage advanced machine learning models to quickly and effectively analyze patient data, leading to early detection of diseases such as cancer or cardiovascular disorders. The real-time capabilities of the model allow for more immediate diagnostic insights, reducing patient waiting times and improving the quality of care. Additionally, this method could be applied in remote and under-resourced areas, providing access to high-level diagnostic tools in regions where specialized expertise is scarce. Ultimately, the proposed system not only augments the decision-making process for clinicians but also contributes to better patient outcomes through more personalized and precise treatment plans.

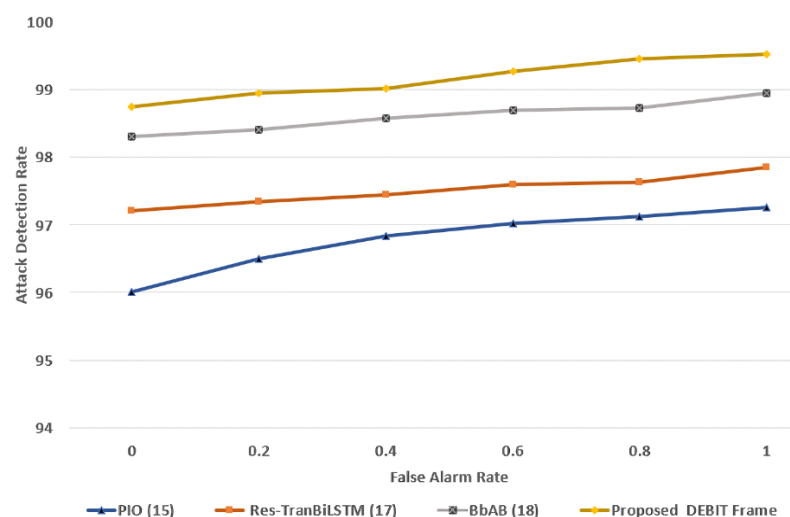


Figure 9. The attack detection rate comparison of suggested method with existing approaches

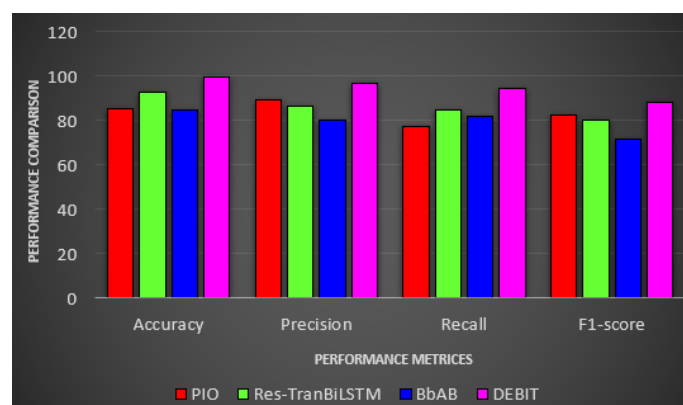


Figure 10. The efficiency comparison of proposed framework with existing frameworks that comprises f1-score, recall, precision, and accuracy

Table 1. The runtime with different epochs comparison of suggested model with other existing models

Techniques	Epoch				
	30	60	90	120	150
PIO [15]	110	185	239	310	389
Res-TranBiLSTM [17]	101	175	246	361	429
BbAB [18]	91	169	224	296	351
DEBIT [proposed]	74	145	196	275	321

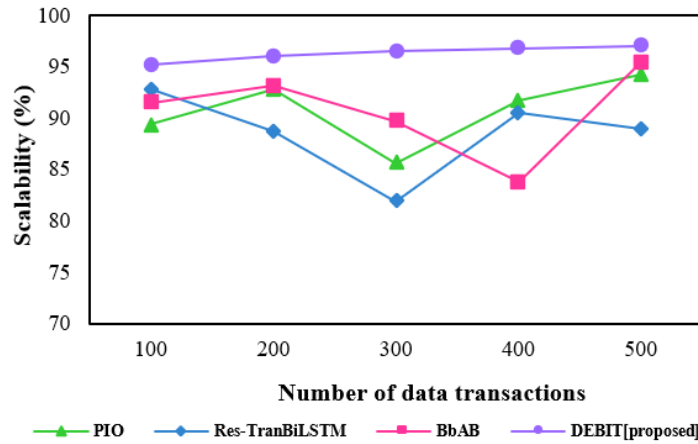


Figure 11. The scalability comparison of suggested method with other existing methods

4. CONCLUSION

In this paper, a DEBIT has been proposed which detects the intrusion using deep learning techniques efficiently. The suggested method's efficiency has been evaluated by a common Bot-IoT intrusion detection dataset. The suggested DEBIT framework has been assessed using MATLAB simulator. Metrics such as recall, precision, F measure, accuracy, and detection rate have been utilized to evaluate the efficacy of the suggested DEBIT approach. According to experimental data, the proposed method has a greater accuracy of 99.5% compared to the 85.4%, 92.5%, and 85% accuracy of existing techniques like PIO, Res-TranBiLSTM, and BbAB. To predict the packet into attack and non-attack. Future plans call for examining various IoT devices, investigating new technologies, and conducting tests using various IoT device data that has been compromised by the hack.

ACKNOWLEDGMENTS

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.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Aarthi Gopalakrishnan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	
Sharon Priya Surendran		✓		✓	✓	✓		✓	✓	✓	✓	✓		
Aisha Banu Wahab	✓		✓	✓	✓		✓		✓	✓	✓		✓	✓

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

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.

INFORMED CONSENT

We certify that we have explained the nature and purpose of this study to the above-named individual, and we have discussed the potential benefits of this study participation. The questions the individual had about this study have been answered, and we will always be available to address future questions.

ETHICAL APPROVAL

The research guide has reviewed and ethically approved this manuscript for publication in this journal.

DATA AVAILABILITY

Data sharing is not applicable to this article as no datasets were regenerated or analyzed during the current study.




REFERENCES

- [1] M. Roopak, G. Yun Tian, and J. Chambers, "Deep learning models for cyber security in IoT Networks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2019, pp. 0452–0457, doi: 10.1109/CCWC.2019.8666588.
- [2] N. Angelova, G. Kiryakova, and L. Yordanova, "The great impact of internet of things on business," *Trakia Journal of Science*, vol. 15, no. Suppl. 1, pp. 406–412, 2017, doi: 10.15547/tjs.2017.s.01.068.
- [3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
- [4] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, no. 1, p. 21, Dec. 2018, doi: 10.1186/s13677-018-0123-6.
- [5] L. Goasduff, "Gartner says 5.8 billion enterprise and automotive IoT endpoints will be in use in 2020," *Gartner Report 2019*, 2020.
- [6] M. Almiari, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, p. 102031, May 2020, doi: 10.1016/j.simpat.2019.102031.
- [7] S. J. Moore, C. D. Nugent, S. Zhang, and I. Cleland, "IoT reliability: a review leading to 5 key research directions," *CCF Transactions on Pervasive Computing and Interaction*, vol. 2, no. 3, pp. 147–163, Oct. 2020, doi: 10.1007/s42486-020-00037-z.
- [8] S. C. Mukhopadhyay and N. K. Suryadevara, "Internet of things: challenges and opportunities," in *Smart Sensors, Measurement and Instrumentation*, 2014, pp. 1–17, doi: 10.1007/978-3-319-04223-7_1.
- [9] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, Jun. 2021, doi: 10.1007/s11831-020-09496-0.
- [10] Y. Li, Y. Zuo, H. Song, and Z. Lv, "Deep learning in security of internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22133–22146, Nov. 2022, doi: 10.1109/JIOT.2021.3106898.
- [11] S. Krishnaveni, P. Vigneshwar, S. Kishore, B. Jothi, and S. Sivamohan, "Anomaly-based intrusion detection system using support vector machine," in *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, 2020, pp. 723–731, doi: 10.1007/978-981-15-0199-9_62.
- [12] R. Uikay and M. Gyanchandani, "Survey on classification techniques applied to intrusion detection system and its comparative analysis," in *2019 International Conference on Communication and Electronics Systems (ICCES)*, Jul. 2019, pp. 1451–1456, doi: 10.1109/ICCES45898.2019.9002129.
- [13] M. Al-Hawawreh, E. Sitnikova, and F. den Hartog, "An efficient intrusion detection model for edge system in brownfield industrial internet of things," in *Proceedings of the 3rd International Conference on Big Data and Internet of Things*, Aug. 2019, pp. 83–87, doi: 10.1145/3361758.3361762.
- [14] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6882–6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.
- [15] A. Shukla, H. Sharma, A. Singh, and A. Ahmad, "Future of internet of things: trends, challenges & insight to artificial intelligence," *International Journal of Advanced Research in Computer Science*, vol. 9, no. Special Issue 2, pp. 162–167, 2018, doi: 10.26483/ijarcs.v9i0.6158.
- [16] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, "IoT intrusion detection taxonomy, reference architecture, and analyses," *Sensors*, vol. 21, no. 19, p. 6432, Sep. 2021, doi: 10.3390/s21196432.
- [17] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach," *Expert Systems with Applications*, vol. 238, p. 121751, Mar. 2024, doi: 10.1016/j.eswa.2023.121751.
- [18] M. Shahin, M. Maghanaki, A. Hosseinzadeh, and F. F. Chen, "Advancing network security in industrial IoT: A deep dive into AI-enabled intrusion detection systems," *Advanced Engineering Informatics*, vol. 62, p. 102685, Oct. 2024, doi: 10.1016/j.aei.2024.102685.
- [19] M. Nanjappan, K. Pradeep, G. Natesan, A. Samyudurai, and G. Premalatha, "DeepLG secNet: utilizing deep LSTM and GRU with secure network for enhanced intrusion detection in IoT environments," *Cluster Computing*, vol. 27, no. 4, pp. 5459–5471, Jul. 2024, doi: 10.1007/s10586-023-04223-3.




- [20] X. Zhang and J. You, "A gated dilated causal convolution based encoder-decoder for network traffic forecasting," *IEEE Access*, vol. 8, pp. 6087–6097, 2020, doi: 10.1109/ACCESS.2019.2963449.
- [21] H. Nandanwar and R. Katarya, "Deep learning enabled intrusion detection system for industrial IOT environment," *Expert Systems with Applications*, vol. 249, p. 123808, Sep. 2024, doi: 10.1016/j.eswa.2024.123808.
- [22] D. Rani and N. C. Kaushal, "Supervised machine learning based network intrusion detection system for internet of things," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2020, pp. 1–7, doi: 10.1109/ICCCNT49239.2020.9225340.
- [23] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975–990, 2020, doi: 10.3745/JIPS.03.0144.
- [24] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.
- [25] G. Kalnoor and S. Gowrishankar, "IoT-based smart environment using intelligent intrusion detection system," *Soft Computing*, vol. 25, no. 17, pp. 11573–11588, 2021, doi: 10.1007/s00500-021-06028-1.
- [26] S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks," *Optik*, vol. 273, 2023, doi: 10.1016/j.ijleo.2022.170419.
- [27] O. A. Alghanam, W. Almobaideen, M. Saadeh, and O. Adwan, "An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning," *Expert Systems with Applications*, vol. 213, 2023, doi: 10.1016/j.eswa.2022.118745.
- [28] Y. Cao, Z. Wang, H. Ding, J. Zhang, and B. Li, "An intrusion detection system based on stacked ensemble learning for IoT network," *Computers and Electrical Engineering*, vol. 110, p. 108836, Sep. 2023, doi: 10.1016/j.compeleceng.2023.108836.
- [29] S. Wang, W. Xu, and Y. Liu, "Res-TranBiLSTM: An intelligent approach for intrusion detection in the internet of things," *Computer Networks*, vol. 235, p. 109982, Nov. 2023, doi: 10.1016/j.comnet.2023.109982.
- [30] V. Saravanan, M. Madijagan, S. M. Rafee, P. Sanju, T. B. Rehman, and B. Pattanaik, "IoT-based blockchain intrusion detection using optimized recurrent neural network," *Multimedia Tools and Applications*, vol. 83, no. 11, pp. 31505–31526, Sep. 2023, doi: 10.1007/s11042-023-16662-6.

BIOGRAPHIES OF AUTHORS






Aarthi Gopalakrishnan    is currently pursuing a Ph.D. at B.S. Abdur Rahman Crescent Institute of Science and Technology. She completed her B.Tech. in Information Technology and M.Tech. in Computer and Communication from Anna University in 2011. She has published and presented several research papers at national and international conferences. She can be contacted at email: aarthig_cse_jan21@crestent.education.



Sharon Priya Surendran    is research work is primarily focuses on cloud computing, image processing, artificial intelligence, and internet of things. She has a rich teaching experience of fourteen years. She has published several research papers in international journals and at conferences. She can be contacted at email: sharonpriya@crestent.education.



Aisha Banu Wahab    research focus is primarily in the area of information retrieval and natural language processing. She has a rich teaching experience of twenty-five years. She has published research papers in peer reviewed journal and conferences. She is a life member of ISTE and a member of ACM. She can be contacted at email: aisha@crestent.education.