International Journal of Computer and Engineering Optimization (IJCEO)
Volume 04, Issue 02, March –April (2026)

RESEARCH ARTICLE

HONEYPOT-ENABLED INTRUSION DETECTION USING OPTIMIZED DEEP LEARNING IN IOT DEVICES

Jeya S Shemona[1, *], Sree Arthi D

[1] Assistant Professor, Department of Electronics and Communication Engineering, Sree Sakthi Engineering College, Karamadai, Coimbatore, Tamil Nadu, India.

[2] Department of Electronics and Communication Engineering, Sree Sakthi Engineering College, Karamadai, Coimbatore, Tamil Nadu, India.

[*]*Corresponding e-mail: jeyashemona.ss@gmail.com*

Abstract – Internet of Things (IoT) based methods have enhanced operations on several applications in the recent year. Cyber-attacks are made more likely by inadequate security protocols in the Internet of Things network. This paper proposed a Honeypot enabled Intrusion Detection using Optimized deep Learning (HIDOL) technique to identify the attack on IoT device. Initially, a honeypot server is placed to find malevolent activity in IoT devices and the patterns are gathered from the attacker. The necessary data are extracted during the feature extraction procedure using a one-hot encoder. By using the Dingo Optimization, the essential features are selected. The Conv-BiLSTM model will classify the vulnerabilities like DDoS attacks, physical attacks and Ransomware attacks. The KDDCUP 19 dataset are used to evaluate the suggested system's efficiency and the evaluation measures like Throughput, Detection Rate and Time efficiency have been utilized to assess the efficacy of the suggested intrusion detection technique. By the comparison analysis the proposed HIDOL archives detection rate of 28.07% which is comparatively higher than the existing system respectively.

Keywords *– Internet of Things, Intrusion Detection, One-hot Encoder, Conv-BiLSTM.*

1. INTRODUCTION

In this modern world the Internet of Things is being used in more sectors. The Internet of Things (IoT) is transforming everyone's lives by offering services like controlling and monitoring connected smart devices [8]. It is a relatively new technology that connects items to the internet to enhance and support people's lives, occupations, and cultures [9]. IoT devices are vulnerable to several possible security issues since they are connected to the internet via immature and insecure communication protocols and software [10]. By utilizing the IoT basic technologies, such as communication technologies, embedded devices, Internet protocols, pervasive and ubiquitous computing, sensor networks, and AI-based applications, gadgets can become smart objects [11]. The main objective is to connect everything so that computers can all become intelligent, programmable devices and more secure means of communicating with one another [12].

Honeypots are a sophisticated software agent and useful instruments for apprehending malevolent attackers. Honeypots are a viable option because they offer useful information about the attackers. A device designed to be attacked and compromised is called a honeypot. With the use of honeypots, hackers are tricked into believing they have physical access to systems [13]. Honeypots can be broadly divided into two types: research honeypots and producing honeypots. Which protect an institution, and research honeypots, which are mostly employed for educational purposes [15]. This study's primary objective is to use honeypots to record attacks on Internet of Things devices. These days, honeypots are available in many shapes and sizes and can be used for a number of purposes. Depending on the degree of involvement with the attacker, it might be categorized [14].

A cyber-attack is a criminal act that interferes with computers and computer networks in order to compromise the security and privacy of individuals and organizations [16]. There are several types of attacks that can be made against different networks using compromised services, including DDoS attacks, Brute force attacks, physical attacks, and ransomware attacks [17]. Attacks have increased everywhere in the world, including in India. Approximately 49,000 cybercrimes were recorded in India in 2018. When it surpassed the 2-lakh barrier in 2020, it saw its first notable surge. In 2021, there were 28 times as many cybercrimes, exceeding the 14-lakh mark [18]. Therefore, a novel, Honeypot enabled Intrusion Detection using Optimized deep Learning (HIDOL) technique have been introduced to maintain the privacy of IoT devices. The suggested work's primary contribution is as follows.

- Initially, a honeypot server is placed to find malevolent activity in IoT devices and the patterns are gathered from the attacker.
- The necessary data are extracted during the feature extraction procedure using a one-hot encoder. By using the Dingo Optimization, the essential features are selected.
- The Conv-BiLSTM model will classify the vulnerabilities like DDoS attacks, physical attacks and Ransomware attacks.
- Finally, the efficiency of the proposed system is assessed using the KDDCUP 19 datasets, and assessment metrics such as Throughput, Detection Rate and Time efficiency are utilized to determine the efficiency of the suggested method in intrusion.

2. LITERATURE REVIEW

In recent years, several research have employed various methodologies to detect intrusions in Internet of Things devices. A few contemporary evaluation techniques and the issues they raise are covered in the section that follows. These are listed in the following order:

In 2020 Pashaei, et al. [1] proposed an industrialized Early Intrusion Detection System (EIDS) to change the Intrusion Detection System (IDS) method. The EIDS, which provides cyber-attacks and industrial network systems protection against vulnerabilities, instantly notifies heads of industrial network security. The attack attains a 98.72% accuracy rate. Improving the security of the IoT environment involves some dangers, which is one of the main disadvantages.

In 2021 Ashiku, and Dagli, [2] suggested a deep learning architecture to create a durable and adaptable intrusion detection system (IDS) that can identify and categorize network threats. Deep neural networks (DNNs) can enable adaptive IDS with the ability to learn to identify recognized. The drawbacks of the detection approach result in slow networks, higher CPU consumption, false positives, and false negatives. For the repartitioned and user-defined multiclass classification, the suggested method yielded an overall accuracy of 95.4% and 95.6%, respectively.

In 2022 Pashaei, et al. [3] proposed a state-action-reward-state action (SARSA) Markov Decision Process (MDP) for honeypot design. By collecting aggressive behaviour, the suggested strategy raises the bar for early honeypot identification. This method archives a highest accuracy rate of 98.15%. Future research trends include the use of alternative RL approaches in conjunction with metaheuristics, which can significantly cut learning time.

In 2020 Chakkaravarthy, et al. [4] proposed a robust Intrusion Detection Honeypot (IDH) to address the cyber-attacks. In a secure test, the suggested IDH is experimentally tested using over 20 different versions of new ransomware. The suggested IDH outperforms an accuracy rate of 96.99% in the ransomware detection system. In future the IDH with transfer learning capabilities will eventually be able to optimize the load on devices with limited resources.

In 2023 Soltani, et al. [5] proposed a framework for deep learning-based IDS to address upcoming attacks. This model is the initial one in the security sector that uses combination of deep novelty-based classifiers and conventional clustering based on the specialized layer of deep structures. This model has an accuracy of 99.85% across the majority of attack types.Future research focus to improve the method based on anomaly traffic.

In 2020 Kaur, and Singh, M, [6] proposed method for signature generation and hybrid intrusion detection based on deep learning. The suggested system detects attacks proactively and efficiently generates signatures, minimizing the harm caused by network attacks. With an accuracy of 99.40% for CICIDS and 99.27% for NSL-KDD datasets, the LSTM surpasses the classifiers in this strategy. By adding more study avenues into the suggested system, this research effort can be improved in the future.

In 2020 Nayyar, et al. [7] suggested a machine learning technique based on LSTMs that uses honeypots to detect unusual network traffic patterns and routes all harmful queries to a black hole server. This technique has been tested and trained on the CICIDS2017 data set, which contains a range of attacks, including patator-based attacks. They provide a 96% reliable abnormality identification method based on LSTM neural networks for effective DDoS assault detection. The need for high-precision floating point arithmetic operations is the model's lone obvious flaw.

3. PROPOSED SYETEM

In this section, Honeypot enabled Intrusion Detection using Optimized deep Learning (HIDOL) technique has been proposed as a way to identify IoT device attacks. Initially, A honeypot server is placed to find malevolent activity in IoT devices and the patterns are gathered from the attacker. The necessary data are extracted during the feature extraction procedure using a one-hot encoder. By using the Dingo Optimization, the essential features are selected. The Conv-BiLSTM model will classify the vulnerabilities like DDoS attacks, physical attacks and Ransomware attacks. Figure 1 shows the proposed HIDOL technique.

3.1. Honeypot Server

An apparatus that logs the attacker's attack strategy is called a honeypot. It does not decrease the force of the attack or stop it. It learns about the attacker by following their movements and gives them the information they ask for. The purpose of the honeypot server is to detect malicious activity on Internet of Things devices and to collect patterns from the attacker. This technique makes use of a Cowrie honeypot to record SSH and Telnet connections. This is where the session's data is recorded. These honeypots are often connected to the Internet in order to continuously monitor the hosts, scripts, and resources that password-guessing attackers use.

3.2. Feature Extraction

In future extraction it will extract the datas from honeypot to detect the threads like DDoS, Ransomware and physical attack. In this the One-Hot Encoder tracks the

attacker's movements and then extracts the necessary features from the data.

3.2.1. One-Hot Encoder

One-hot encoding, also known as bit-effective coding. This method is applied in a machine-learning model to encode category variables into numeric values. Applying numerical data makes deep learning techniques and machine learning more accessible. In this the vector representation for every system call and a unique system call for every place. As a result, different numbers of system calls correlate with varied input vector sizes.

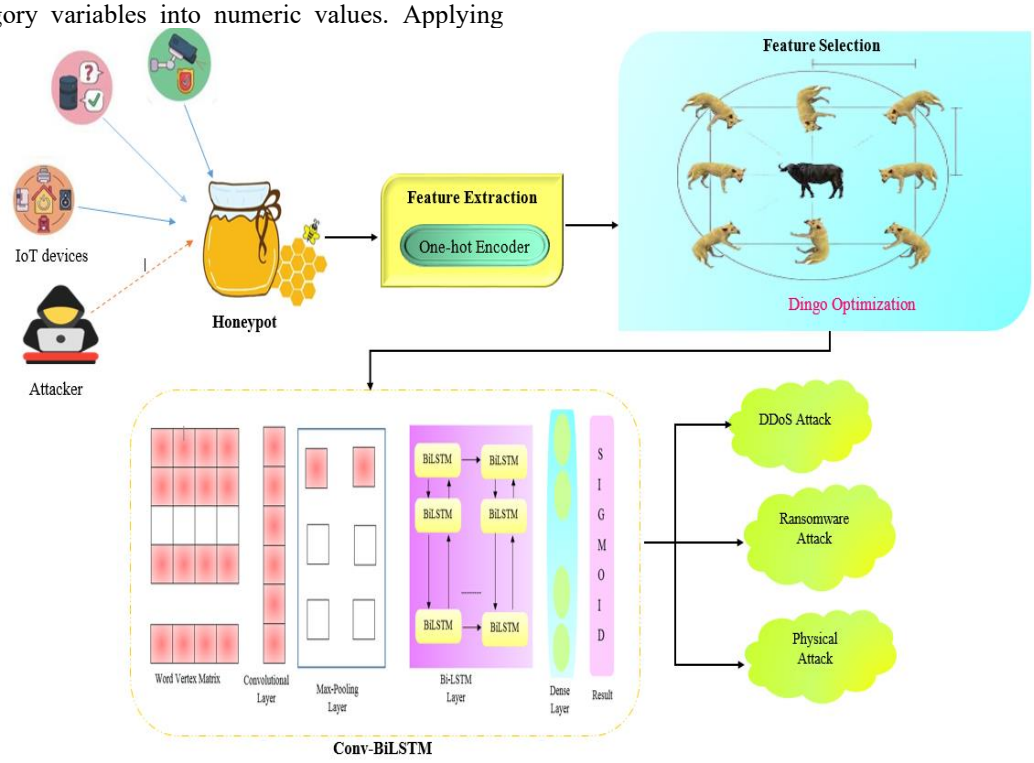

Figure 1. Workflow of the proposed HIDOL Technique.

3.3. Improved Dingo Optimization

Improved Dingo Optimization's (IDO) optimization model is made for feature selection, which optimizes data and provides pertinent features. Finding the best real-world system solutions is a difficult task. Because there are multiple excellent solutions available. The improve persecution, scavenging, group attack, and survival are shown in equation (1)-(2).

$$\propto= (BF - WF) \tag{1}$$

$$X = \frac{mean\ (X(F-WF))}{mean\ (X(F-BF))} \tag{2}$$

$$CB = \propto \times \left(\frac{P}{X}\right) \tag{3}$$

The best and worst objective functions are denoted by the terms BF and WF, respectively, in this instance. Fitness is represented by F, distance by A, generality by X and p, and arbitrarily by CB, which is a number between 0 and 1.

3.4. Conv BiLSTM Layer

The Conv-BiLSTM model is used to classify the data source assault. The framework of the proposed model is described in the following section. The five steps that comprise the Conv-BiLSTM model's higher levels structure.

3.4.1. Word Vectorization

The system eventually converts the outcome of the selecting features process into discrete words or tokens. This converts every token into the numerical representation of a vector. GloVe and Word2Vec, two pre-trained word-embedded models, are employed to create the word vector matrix. The model's accuracy is evaluated using the Word2Vec and GloVe models. The input text can be expressed by $P = \{a_1, a_2 \dots \dots \dots a_n\}$, where a_1 through a_n are word vectors with length f, and P indicates the length n.

$$P = a_1, a_2 \dots \dots \dots a_n \in R^{n*f} \tag{4}$$

Although the lengths of the input texts may vary, every output text should be the same length (l). No padding was used to lengthen its length. Text that exceeds the allowable length, l, will be chopped off. However, if the text is shorter than length (l), no more paces are added to the total. This results in a uniform matrix dimension for all texts. Any -dimensional text has the following definitions:

$$P = a_1, a_2 \dots \dots \dots a_n \in R^{i*f} \tag{5}$$

3.4.2. Convolutional Layer

The primary level of the CNN model, the convolution layer, is excellent at determining which words are most important in a phrase. The layer of one-dimensional convolution created from the word embedding step receives

the data set $P \in R^{i*f}$ of word vectors. To create the local feature of an n-gram, a convolution word vector matrix with N filters and a convolution kernel width of q is constructed in a one-dimensional convolution layer.

$$e_i^m = f(a^m \otimes X_{i:i+a-1} + T^m) \quad (6)$$

The weight matrix a represents the word vector dimension d, the convolution process, and T^m the bias of the filter F_n.

3.4.3. Max-Pooling Layer

The convolution method creates the feature maps, while the pooling layer selects the best properties, $m = \max\{m\}$, to compute the local acceptable statistics. To deliver a single output containing the maximum number. One-dimensional max-pooling is used to aggregate a down-sampled representation of the original input and its kernels. By efficiently reducing the number of features, the CNN model avoids overfitting and speeds up training while simplifying parameter tweaking.

3.4.5. BiLSTM Layer

In a departure from LSTM, Bi-LSTM employs hidden states to facilitate information flow in both directions. It might enhance the ability of Bi-LSTMs to recognize contextual cues. Using these bidirectional links, it is possible to Maintain input data that comes from the past and the future, rather than requiring decay to integrate future information as is the case with the usual RNN model. Typically, a Bi-LSTM is built by linking the outputs of two competing LSTM networks. The Bi-LSTM will proceed to weigh the results.

3.4.6. Dense Layer and Result

A dense layer in this approach uses values to connect the inputs and outputs. In the last layer, the final output is generated using a function called a sigmoid. The average generated at random is translated to binary format. Equation (7) depicts the sigmoid function's predictive performance.

$$R = Sigmoid\ (uf + q) \quad (7)$$

Binary cross-entropy can be used to classify the data as either 0 or 1 based on the sentiment analysis result. In this study, a negative perspective is represented by a score of 0 and a positive perspective by a score of 1.

4. RESULT AND DISCUSSION

4.1. Description of the dataset

KDDCUP 19 Dataset

This dataset was created using information from the 1998 DARPA IDS evaluation program and utilized in the third global Competition for Knowledge Development and Data Mining Tools. The KDD-Cup dataset contains 41 dimensions in total. There are 31279 KDD Cup instances and 33746 ISCX instances in the used subset.

4.2. Description of evaluation matrices

Throughput

Throughput is the actual bandwidth measured at that precise instant during file transmission. In contrast to bandwidth, that is generally stated in bits per second (bps), throughput more properly represents the actual bandwidth over a certain time period and under specific network conditions, particularly when downloading a specific item. It is calculated by dividing the total quantity of data (in bits) successfully conveyed by the total amount of time (in seconds) over which the data was transmitted.

$$Throughput = \frac{Total\ number\ of\ transmitted\ data}{Total\ time\ to\ trasmit\ a\ data} \quad (8)$$

Packet Loss

The percentage of frames dropped throughout data transmission is referred to as packet loss. Packet loss is an important metric to know how many packets are lost. Network collisions and congestion are the causes of this. It is computed in the following format:

$$Packet\ Loss = \frac{Amount\ of\ loss\ pocket}{Total\ number\ of\ packet\ send} \times 100 \quad (9)$$

Detection Rate

The Detection Rate (DR) is a vital measure of the system's ability to consistently identify attacks from all positive occurrences. IDPS is critical to cybersecurity, especially in terms of attack prevention. The following formula is used to obtain the detection rate:

$$Detection\ Rate = \frac{True\ Positive}{True\ Positive + False\ Positive} \quad (10)$$

Performance of Throughput

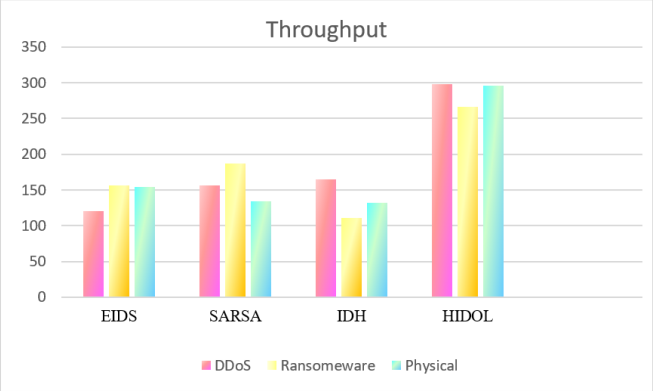

Figure 2. Throughput on Attacks

Figure 2 describes the throughput on attacks. The suggested HIDOL is contrasted with existing techniques like EIDS, SARSA, and IDH. This method archives the highest throughput value when compared to other existing techniques.

Detection Rate

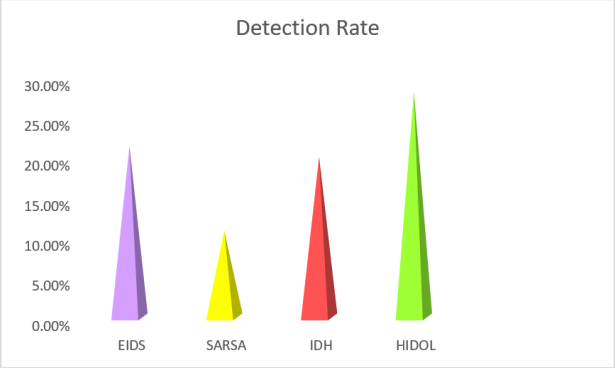

Figure 3. Comparison of Detection rate

Figure 3 illustrates the proposed and current systems' detection rates using the dataset. With a detection rate of 28.07%, the proposed HIDOL archives outperform the current system in comparison.

Time Efficiency

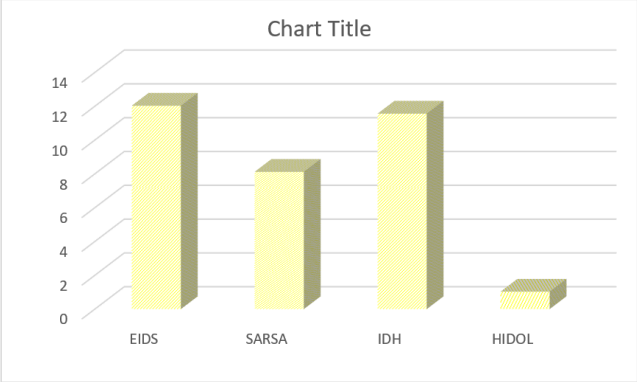

Figure 4. Quickly and effectively vulnerabilities in a system

Figure 4 displays how quickly and effectively vulnerabilities in a system or IoT devices may be found and examined is referred to as time efficiency in vulnerability detection. The proposed HIDOL systems time of 1.03 milliseconds is quick compared to EIDS, SARSA and IDH which takes 12.03, 8.12 and 11.54 respectively.

5. CONCLUSION

In this paper a Honeypot enabled Intrusion Detection using Optimized deep Learning has been suggested as a way to identify the attack in IoT devices. A honeypot server is placed to gather the patterns from the attackers. In this the necessary data are extracted during the feature extraction procedure using a one-hot encoder. By using the Dingo Optimization, the essential features are selected. The Conv-BiLSTM model will classify the vulnerabilities like DDoS attacks, physical attacks and Ransomware attacks. KDDCUP 19 datasets are employed to assess the suggested system's efficiency. The proposed system is evaluated using python programming. Evaluation measures like Throughput, Detection Rate and time efficiency have been employed to assess its effectiveness of the recommended intrusion detection method. The suggested HIDOL archives rate for identification is 28.07%, which is greater than the current system in comparison. In future this research focus on increases the performance more than this using optimization process.

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

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to the supervisor and faculty members for their valuable guidance and continuous support throughout this research work.

REFERENCE

[1] A. Pashaei, M. E. Akbari, M. Z. Lighvan, and H. A. Teymorzade, “Improving the IDS performance through early detection approach in local area networks using industrial control systems of honeypot”, In 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), IEEE, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] L. Ashiku, and C. Dagli, “Network intrusion detection system using deep learning”, *Procedia Computer Science*, vol. 185, pp. 239-247, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] A. Pashaei, M. E. Akbari, M. Z. Lighvan, and A. Charmin, “Early Intrusion Detection System using honeypot for industrial control networks”, *Results in Engineering*, Vol. 16, pp. 100576, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] S. S. Chakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi, and B. Raman, “Design of intrusion detection honeypot using social leopard algorithm to detect IoT ransomware attacks”, *IEEE Access*, vol. 8, pp. 169944-169956, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] M. Soltani, B. Ousat, M. J. Siavoshani, and A. H. Jahangir, “An adaptable deep learning-based Intrusion Detection System to zero-day attacks”, *Journal of Information Security and Applications*, vol. 76, pp. 103516, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] S. Kaur, and M. Singh, “Hybrid intrusion detection and signature generation using deep recurrent neural networks”, *Neural Computing and Applications*, vol. 32, pp. 7859-7877, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] S. Nayyar, S. Arora and M. Singh, "Recurrent Neural Network Based Intrusion Detection System," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] 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. [CrossRef] [Google Scholar] [Publisher Link]
[9] B. Susilo, and R. F. Sari, "Intrusion detection in IoT networks using deep learning algorithm", *Information*, vol. 11, no. 5, pp. 279, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[10] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review", *Applied sciences*, vol. 11, no. 18, pp. 8383, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[11] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, Solutions and future directions", *Electronics*, vol. 9, no. 7, pp. 1177, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[12] Sicato, S., Costa, J., Singh, S.K., Rathore, S. and Park, J.H., 2020. A comprehensive analyses of intrusion detection system for IoT environment. Journal of Information Processing Systems, 16(4), p.975. [CrossRef] [Google Scholar] [Publisher Link]
[13] A. Pashaei, M. E. Akbari, M. Zolfy Lighvan, and A. Charmin, "Deep Learning Based Early Intrusion Detection in IIoT using Honeypot", *Majlesi Journal of Electrical Engineering*, vol. 17, no. 2, pp. 69-77, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[14] S. P. RM, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture", *Computer Communications*, vol. 160, pp. 139-149, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[15] A. P. Wahyu, K. Fauziah, A. S. Nahrowi, M. N. Faiz, and A. W. Muhammad, "Strengthening Network Security: Evaluation of Intrusion Detection and Prevention Systems Tools in Networking Systems", *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 9, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[16] R. Vishwakarma, and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks", In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, April, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[17] R. K. Shrivastava, B. Bashir, and C. Hota, "Attack detection and forensics using honeypot in IoT environment", In Distributed Computing and Internet Technology: 15th International Conference, ICDCIT 2019, Bhubaneswar, India, Proceedings 15, Springer International Publishing, January 10–13, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[18] S. Krishnaveni, S. Sivamohan, S. Sridhar, and S. Prabhakaran, "Network intrusion detection based on ensemble classification and feature selection method for cloud computing", *Concurrency and Computation: Practice and Experience*, vol. 34, no. 11, pp. e6838, 2022. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Jeya S. Shemona is an Assistant Professor with 4 years of teaching experience in the field of Electronics and Communication Engineering. She earned her Ph.D. from Anna University with a specialization in Computer-Aided Diagnosis Systems for the early detection of cancer in red blood cells using image processing and deep learning techniques.
Her areas of expertise include Image Processing, Machine Learning, Pattern Recognition, Deep Learning, and Medical Image Analysis. She has published research papers in reputed journals, authored the book Computer Aided Diagnosis System for Early Detection of Cancer in Red Blood Cells, and serves as a reviewer for the Journal of Imaging Informatics in Medicine. She also holds a published patent for a solar panel cleaning robot for industrial solar power plants.
Dr. Shemona is actively involved in academic research, innovation, faculty development programs, and technical conferences. Her commitment to quality education and research excellence continues to contribute to advancements in engineering and emerging technologies.

Sree Arthi D M.E**,** is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering at Sree Sakthi Engineering College, Karamadai, Tamil Nadu, since 4 June 2025. She has rich academic and industrial experience in the fields of Electronics and Communication Engineering, Automotive Embedded Systems, and Communication Networks.
Prior to joining academia, she worked as an Embedded Consultant at L&T Technology Services, Bengaluru, and as a Software Integrator at Bosch Global Software Technologies Private Limited for Audi and Porsche projects. She has expertise in automotive software integration, embedded software development, software testing, and automotive tools and technologies.
She has published one research article in an international journal and presented ten papers at national and international conferences. She is an active member of the Indian Society for Technical Education (ISTE), and the Computer Society. Her research interests include Automotive Embedded Systems, Digital Communication, Computer Networks, Wireless Communication, and Embedded System Design.
She is passionate about teaching, research, and lifelong learning and actively participates in academic, technical, and professional development activities. She is committed to mentoring students and contributing to technological innovation and excellence in engineering education.

Arrived: 13. 03. 2026
Accepted: 19. 04. 2026