

# Cloud computing environment based hierarchical anomaly intrusion detection system using artificial neural network

Mangalapalli Vamsikrishna<sup>1</sup>, Garapati Swarna Latha<sup>2</sup>, Gajjala Venkata Ramesh Babu<sup>3</sup>,  
Koppiseti Giridhar<sup>4</sup>, Lakshmeelavanya Alluri<sup>5</sup>, Giddaluru Somasekhar<sup>6</sup>,  
Bhimunipadu Jestadi Job Karuna Sagar<sup>7</sup>, Naresh Dondapati<sup>8</sup>

<sup>1</sup>Department of Computer Applications, Aditya University, Kakinada, India

<sup>2</sup>Department of Computer Science and Engineering, Rajamahendri Institute of Engineering and Technology, Rajamahendravaram, India

<sup>3</sup>Department of Computer Science (MCA), Sri Venkateswara University College of Commerce, Management and Computer Science, Sri Venkateswara University, Tirupati, India

<sup>4</sup>Department of Computer Science and Technology, Madanapalle Institute of Technology and Science, Madanapalle, India

<sup>5</sup>Department of Computer Science and Engineering, Sagi Rama Krishnam Raju Engineering College, Bhimavaram, India

<sup>6</sup>Department of Computer Science and Engineering, Gandhi Institute of Technology and Management (Deemed to be University), Hyderabad, India

<sup>7</sup>Department of Computer Science and Engineering, Joginpally B. R. Engineering College, Hyderabad, India

<sup>8</sup>Department of Electronics and Communication Engineering, Lakireddy Balireddy College of Engineering, Mylavaram, India

## Article Info

### Article history:

Received May 8, 2024

Revised Aug 31, 2024

Accepted Oct 1, 2024

### Keywords:

Anomalous activities

Artificial neural network

Big data analytics

Intrusion attacks

Intrusion detection system

Malicious actions

## ABSTRACT

Nowadays, computer technology is essential to everyday life, including banking, education, entertainment, and communication. Network security is essential in the digital era, and detecting intrusion threats is the most difficult problem. As a result, the network is monitored for unusual activity using this hierarchical anomaly intrusion detection system, and when these actions are detected, an alert is generated. This hierarchical anomaly intrusion detection system, which uses artificial neural network (ANN) and is implemented on a cloud computing environment, analyzes data even in the high levels of traffic and protects computer networks and data from malicious activity. As a result, this system shows better detection, accuracy, and precision rates.

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



## Corresponding Author:

Mangalapalli Vamsikrishna

Department of Computer Applications, Aditya University

Surampalem, Kakinada, Andhra Pradesh 533005, India

Email: vkmangalampalli@gmail.com

## 1. INTRODUCTION

Internet of everything was the previous term for the internet of things (IoT). Physical objects can perceive, store, analyze, and send data over the Internet without interruption from machines or people due to the IoT. These applications and services are developing quickly, even in everyday household products. Data collection, processing, and transfer to applications is the primary goal of the IoT [1]. Data collection, processing, and data transfer are handled by application processes and tiny, memory-constrained sensors and devices. There is wireless fidelity (Wi-Fi), Bluetooth, ZigBee, Bluetooth low energy (BLE), and so on. Device deployment is essential for maintaining network security and data safety in terms of security and privacy.

Among the many issues of the IoT, one of the most important is ensuring security and privacy because wireless technology, which is more vulnerable to network attacks, is used for data transfer. An attacker's soft target has become the IoT network because to the increasing demand for IoT and connected,

heterogeneous objects and devices. fog network layer gateway, wired/wireless network perception layer sensors, application layer personalized based services support layer cloud [2].

In addition, since many IoT nodes exchange and store private information, attackers have found them to be easy targets. As a result, it needs a lightweight algorithm that is different in nature to complete the task. IoT systems have a four-layered design [3]. While intrusions can be placed in any one or more of the IoT's layers, the network layer is the most vulnerable. When anything in a system deviate from its normal behavior, an intrusion detection system (IDS) increases an alarm, this is an essential component of an internet of things intrusion detection system.

This includes four main methods: hybrid, anomaly, specification, and signature-based systems. When anything departs from a system's regular profile, anomaly-based IDS send alerts. Although it causes a lot of false alarms, it works best against unknown attacks [4]. However, signature-based IDS utilize the pattern, signature, and behavior of known attacks and raise an alert when any matches are discovered. It does not identify unknown assaults and is primarily appropriate for recognized attacks. IDS based on specifications can only identify some types of attacks and are challenging to create and validate [5].

On the other hand, hybrid-based IDS combines the three. Due to daily novel attacks that follow no set pattern, the security and privacy of internet of things systems are not sufficiently secured by traditional IDS, which makes artificial intelligence-internet of things (AI-IoT) architecture with self-healing and self-corrective capabilities necessary. AI can function as a decision-making brain in this combination, while IoT can function as a nervous system that carries out the predetermined action against the attack. Cloud-based IoT, which can solve connectivity, storage capacity, and data computation issues, has increased in popularity as a result of IoT's limited computational power and storage capacity [6].

When cloud-based internet of things and artificial intelligence systems are combined, it becomes easier to respond on specific data and create systems that can make the right decisions under particular conditions. Machine learning (ML) in AI helps to reduce any node's analysis time. A camera operating as a sensor in the IoT, for instance, would submit every image for analysis. However, a camera with inbuilt ML would only send images containing a specified object for study. It reduces down on analysis time by supplying only frames of images that match. Thus, in the least amount of time, machine learning algorithms produce better results for intrusion detection [7]. Machine learning has emerged as the most effective method for transforming data into knowledge in the twenty-first century. It can quickly identify particular trends and patterns from huge amounts of multidimensional, multidimensional information. It is the most accurate way to find network intrusions. Cloud-based data centers offer a range of services, including software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS), ensuring customers are flexible, easily available, and better services. For handling the networking aspects of complicated quality of service (QoS) requirements in the cloud, an increasingly popular choice is the software-defined networking (SDN) network [8].

Adequate cyber security and protection for cloud services without compromising quality of service and maintaining a sufficient level of openness is another essential component of the networking infrastructure. Despite its outstanding ability in managing different traffic types with different quality of service demands, SDN is lacking integrated security features. To secure data transmitted across the networks, further security layers are needed, much like in traditional networks. Firewalls, access control lists (ACLs), antivirus applications, encryption, and other security measures are common preventive defenses [9]. However, security issues remain and intrusions can still happen even with a robust defense line. IDS and other additional reactive security techniques thus become necessary. While network-based intrusion detection systems (NIDS) directly get data from the network through packet examination, IDS identify intrusions by evaluating system data. All packets are analyzed by traditional IDS like Suricata and Snort. However due to the huge amount of data, this causes the network to operate worse, increasing delay and adding more processing cost to the infrastructure [10]. Therefore, the research gaps observed from below literature survey are accuracy, precision and detection rate.

Following is the arrangement of the remaining content in the article included in section 2 is literature survey. Section 3 presents the architecture of the cloud computing environment based hierarchical anomaly intrusion detection system using artificial neural network (ANN). In section 4 explains result analysis and section 5 concludes the paper.

## 2. LITERATURE SURVEY

In this paper, they propose an intrusion detection system to detect and recognize different types of attacks, based on machine learning and state observer. The detection system picks up on anomalies in both the physical states of the trains and the data from the wireless network. There are two layers in this method [11]. Using machine learning algorithms, the first layer detects and identifies wireless network attacks. Based

on a state observer, to determine the anomalous physical state of train operation, the second layer is used. The results of the simulation demonstrate that the useful and successful the proposed approach.

For the field control system in industrial process automation, a novel multimodel-based anomalous intrusion detection system with embedded intelligence and resilient coordination is created [12]. For the system, a multimodel-based anomaly detection technique is suggested, and related intelligent detection algorithms are created. Finally, an extensive evaluation of the selected IDS real-time performance and detection accuracy is carried out utilizing an optimized performance network engineering tool on a combined simulation platform. High precision and good real-time capabilities are two areas in which the suggested system performs, as the experimental results clearly demonstrate.

A novel approach on linear systems theory-based intrusion detection for reconfigurable network routing. They can differentiate between different types of routing attacks by taking into consideration the z-plane poles of the system [13]. They can thought of the z-plane as a naturally occurring two-dimensional feature space. The new linear systems perspective as the basis for two different host-based intrusion detection techniques, which are presented and examined through a case study.

Based on the technique of self-generated coding, an intrusion detection approach is provided. In contrast to the current detection methods that depend on pseudorandom coding generators; by using an authentication mechanism, the suggested method generates a multiplicative coding scheme on its to be used. This indicates that by parsing the most recent timestamp that is accessible online, the original train measurement data's encrypting and decrypting coding sequences are dynamically updated. By preventing the attacker from identifying the coding sequences before they are used, this enhances the train-ground communication network's data transmission security [14].

In order to enhance system-wide situational awareness, a mechanism for integrating real-time data from the physical and cyber domains is developed in this work. It is shown how enhanced situational awareness might contribute to a decrease in intrusion detection of false positives. Different feature transformation and selection methods are used to handle the explosion of the cyber-physical state space that results from combining physical and digital data. An application that represents real-world data sources seen in a utility by gathering cyber and power system telemetry from many sensors, combines our fusion engine even more into a testbed for cyber-physical power systems [15].

A hybrid model is suggested to find anomalies in integration cloud service (ICS) setups. To generate a signature database, it utilizes a Bloom filter, an updated nearest-neighbor rule algorithm for dataset balance, dimensionality reduction algorithms for anomaly identification, and preprocessing approaches to normalize and scale data. To identify novel attacks, the hybrid approach combines detection at the package contents level with an additional instance-based learner [16].

In order to represent global application behavior, an IDS model that integrates many detection methods into a single system is provided by the research. It suggests a modified system called graph, which combines detection methods using a deep neural network [17]. Verified on three datasets with various levels of complexity, the study demonstrates improved detection results, higher detection rates, and less false positives.

In order to decrease false detection rates and increase detection accuracy, the authors suggest a local outlier factor (LOF)-based intrusion detection approach that uses voltage signals on controller area network (CAN) buses. This method is the first for real-vehicles bus-off intrusion detection because it does not require changing the CAN protocol or adding more computational burden. The method also reduces the false detection rate [18].

In order to solve data imbalance and enhance the functionality of current systems, this study suggests a unique AI-based anomaly detection system [19]. Reconstruction error, Wasserstein distance-based generative adversarial networks, and small attack traffic are all supported by the system's advanced generative model, which utilizes autoencoder-driven deep learning models to generate synthetic data. Improving the accuracy of network threat detection is the aim of this approach.

Without requiring restricted data access or changing the architecture of the electronic control unit (ECU), attacks are eliminated by the novel unsupervised intrusion prevention system (IPS) for vehicle CANs. To identify fuzzing and spoofing attacks, the system utilizes two machine learning methods, the most accurate of requires lowest number bytes of data [20]. The system attains above 99% accuracy, 97% F1-scores, and less than 80  $\mu$ s detection times. The only method that can get removal of attacking frames before damage is done with this type of approach.

Using binary and multiclass classification, to enhance network intrusion detection, the system in use is a hybrid convolutional neural network (CNN) and bidirectional long short-term memory (BiLSTM). The most popular datasets were utilized to test and evaluate the suggested model's efficiency. Furthermore, they made use of the SDN dataset, which is dedicated only to SDN [21]. The results show the success that the suggested model is at obtaining high accuracy while requiring lesser training time.

By detecting attacks each time a packet is received, the suggested approach reduces system load and allows for real-time detection. In comparison to traditional techniques, it reduces memory access increases to

less than 30% [22]. In addition, to providing high classification performance of hardware-based approaches, the software-based solution offers outstanding scalability and adaptability against a range of threats, enabling it to detect and prevent different cyber-attacks.

Dynamic-weighted aggregation federated learning (DAFL), an effective intrusion detection method that utilizes federated learning. In particular, DAFL has preserved data privacy by utilizing all of the benefits of federated learning. Furthermore, our approach has dynamically implemented weighting and filtering algorithms for local models, as compared to a traditional federated-learning based intrusion detection system [23]. DAFL can identify network intrusions more effectively and with less communication overhead in this manner. They provide comprehensive designs for DAFL, and our test results show that DAFL can maintain data privacy while achieving good detection performance with minimal network communication overhead.

In this article, they will create a framework to evaluate and apply network security techniques while keeping track of each device connected to the network and its attack rate. Subsequently, different options will be offered for protecting the cloud server against intrusions [24]. Several factors will be used at the end of the paper to evaluate the accurate the results, and each conclusion will be used as a framework, the compared value of the results from this research will be determined.

In order to identify malicious anomalies that pose a threat to the network, at the unmanned aerial vehicles (UAVs) and ground station levels, an advanced intrusion detection and response technique runs. This approach involves the proposal of a collection of detection and response mechanisms to monitor the behaviors of UAVs and classify them into normal, abnormal, suspicious, and malicious categories based on the cyber-attack that has been detected [25]. They concentrate on the lethal cyberattacks that can affect a UAV network: spreading false information, jamming, global positioning system (GPS) spoofing, and black hole and gray hole attacks.

### 3. METHOD

In this section, the frame of cloud computing environment based hierarchical anomaly intrusion detection system using ANN is observed. In Figure 1, the dataset is collected as input. The data undergoes pre-processing, and features are then extracted from the pre-processed data, the data is given to flow aggregator. The flow-based IDS “anomaly detection engine” is applied to the data in flow aggregator. After, the IDS based on flow training data and testing data are the two categories into which the data is divided. The train set is given to train model as well as test set is given to ANN classifier. Finally, the performance of the model is evaluated.

The process of finding and fixing (or eliminating) incorrect or incomplete records from a dataset is known as data preprocessing, preparation, or cleaning. It involves determining whether sections of the data are incomplete, inaccurate, or irrelevant, and then changing, replacing, or deleting the coarse data. Data preparation is the process of converting unprocessed data into an understandable format. This essential phase of data mining occurs since we are unable to operate with raw data. In feature extraction, raw data is transformed into numerical features while maintaining the information in the original data set. Important features are then chosen from the dataset. These feature sets will help in the classifier's ability to understand record behavior and patterns for both common and attack packet types. Any classifier will lead to performance due to improper feature selection. The behavior and pattern of new packets will be predicted with the help of the feature classifier. As a result, learning will happen quickly and attack prediction accuracy will increase. The goal of feature extraction is to extract as much the relevant data as possible while reducing the complexity of the data sometimes referred to as “data dimensionality.” This improves the process of analysis and enhances the effectiveness and efficiency of machine learning algorithms.

In the SDN network, the flow aggregator is in charge of collecting port and flow information from OpenFlow switches. This module retrieves flow, port, and aggregated information from the switches by sending periodic queries through the controller. Reply event messages are returned by OpenFlow switches. In the port statistics reply, information about packets sent and received, bytes, dropped packets, errors related to the cyclic redundancy check (CRC) and frames, and collisions, are included; in the aggregate statistics reply, the total aggregated byte count and the packet count handled by a switch are included. In addition to information on the protocol, byte and packet counts, duration, source and destination media access control (MAC) and internet protocol (IP) addresses are also included in the flow statistics reply.

In the suggested IDS design, the first line of defense is the flow-based IDS. The datasets comprise network traffic that is both normal and malicious. Malicious traffic that is contained in the dataset is found by the IDS. The difference between the actual and detected number of attacks by an IDS is used to evaluate the effectiveness of the system. It functions on all incoming network traffic. The detection algorithm is based on an anomaly-based scheme. Any suspicious action that differs from your established normal patterns of behavior is detected by anomaly detection. The data is used to produce a train set and a test set. To be more

precise, training data is the dataset that you utilize to train your algorithm or model to make correct predictions about your results. The purpose of validation data is to assess and direct the parameters and algorithm you choose for your model. Testing datasets are used to evaluate the accuracy and performance of the developed model.

The data is provided to the ANN classifier after the trained model. Modeling complex patterns and predicting problems, ANN algorithms are based on brain function. An approach to machine learning for categorization issues is the artificial neural network. A weighted set of connected input-output networks is called an ANN. Each connection has a specific weight assigned to it. It has three layers: one for input, one or more for intermediate, and one for output. The data is then evaluated.

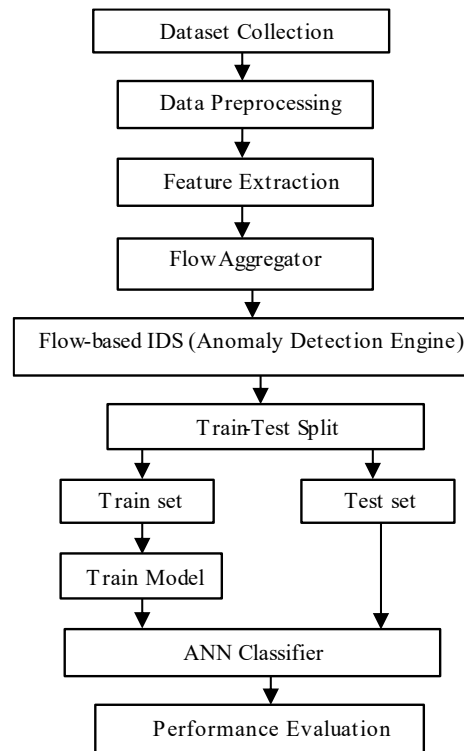


Figure 1. Frame of cloud computing environment based hierarchical anomaly intrusion detection system using ANN

#### 4. RESULT ANALYSIS

In this section, the performance analysis of frame of cloud computing environment based hierarchical anomaly intrusion detection system using ANN is observed. In Table 1, ANN and decision trees are used to analyze the performance of a hierarchical anomaly intrusion detection system based on cloud computing environments. Accuracy, precision, and detection rate are measured for ANNs. Because ANN is used in a cloud computing environment by this hierarchical anomaly intrusion detection system. It analyzes data even in high levels of traffic and protects computer networks as well as data from malicious activity.

Table 1. Performance analysis

Parameters	Decision tree (DT)	ANN
Accuracy	91.3	98.5
Precision	85.4	92.7
Detection Rate	78.6	89.1

In Figure 2, accuracy comparison graph is observed. The comparison is between decision tree and ANN. ANN shows high accuracy for cloud computing environment based hierarchical anomaly intrusion detection system using ANN. As attacks will can be detected accurately by using ANN. Precision comparison graph is observed in Figure 3. The decision tree and ANN is compared for precision. The

precision shows higher for cloud computing environment based hierarchical anomaly intrusion detection system using ANN. Graphical representation of detection rate efficiency is compared between decision tree and ANN is observed in Figure 4. ANN shows higher efficiency detection rate for cloud computing environment based hierarchical anomaly intrusion detection system using ANN. Attacks are detected accurately and fast by using this system.

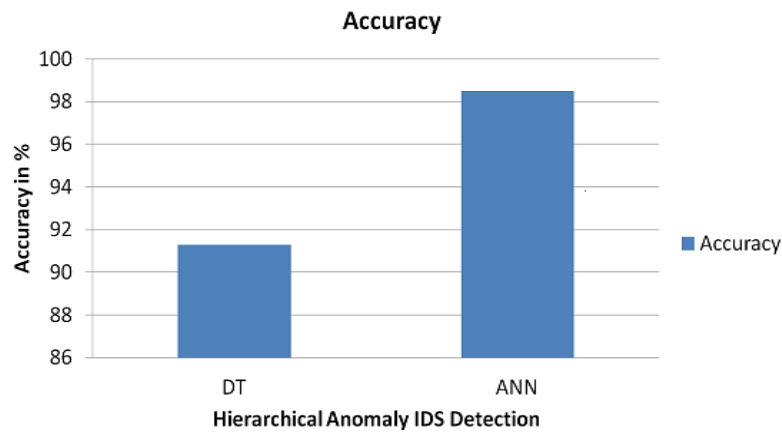


Figure 2. Accuracy comparison graph

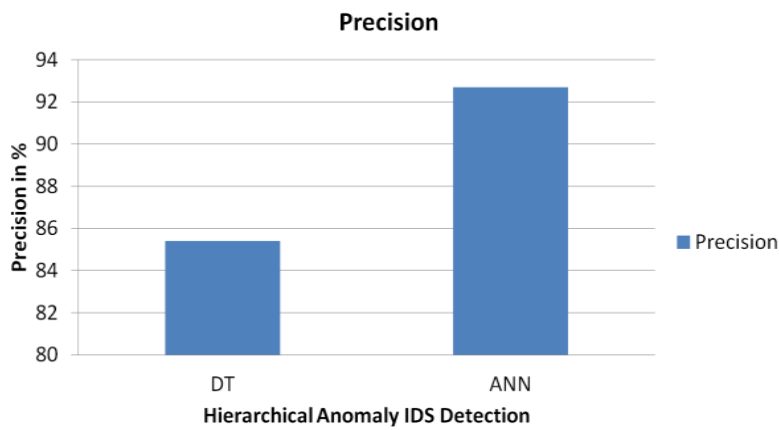


Figure 3. Precision comparison graph

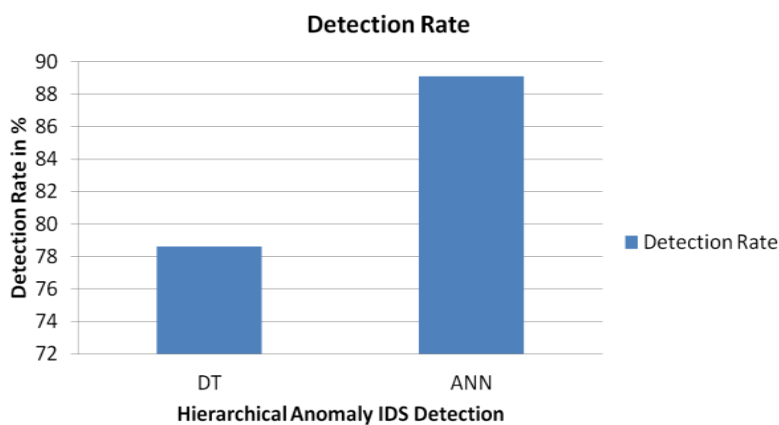


Figure 4. Efficiency comparison graph

## 5. CONCLUSION

In this section, cloud computing environment based hierarchical anomaly intrusion detection system using ANN for utilizing the advantages of each intrusion detection scheme and addressing its drawbacks at the next level of the hierarchy to create a comprehensive, robust intrusion detection system by integrating many categories of intrusion detection techniques hierarchically. As a result, the network is monitored for unusual activity using this hierarchical anomaly intrusion detection system, and when these actions are detected, an alert is generated. This anomaly intrusion detection system is hierarchical, which uses ANN and is implemented on a cloud computing environment, analyzes data even in a context of high levels of traffic and secures computer networks and data from malicious activity. Thus, in terms of accuracy, precision, and detection rate, this system performs better.





## REFERENCES

- [1] M. A. Siddiqi and W. Pak, "Tier-based optimization for synthesized network intrusion detection system," *IEEE Access*, vol. 10, pp. 108530–108544, 2022, doi: 10.1109/ACCESS.2022.3213937.
- [2] Y. Sun, L. Hou, Z. Lv, and D. Peng, "Informer-based intrusion detection method for network attack of integrated energy system," *IEEE Journal of Radio Frequency Identification*, vol. 6, pp. 748–752, 2022, doi: 10.1109/JRFID.2022.3215599.
- [3] T. Wisanwanichthan and M. Thammawichai, "A double-layered hybrid approach for network intrusion detection system using combined naive Bayes and SVM," *IEEE Access*, vol. 9, pp. 138432–138450, 2021, doi: 10.1109/ACCESS.2021.3118573.
- [4] R. Bitton and A. Shabtai, "A machine learning-based intrusion detection system for securing remote desktop connections to electronic flight bag servers," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1164–1181, May 2021, doi: 10.1109/TDSC.2019.2914035.
- [5] J. Cui *et al.*, "Collaborative intrusion detection system for SDVN: a fairness federated deep learning approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 34, no. 9, pp. 2512–2528, Sep. 2023, doi: 10.1109/TPDS.2023.3290650.
- [6] T. Kim and W. Pak, "Early detection of network intrusions using a GAN-based one-class classifier," *IEEE Access*, vol. 10, pp. 119357–119367, 2022, doi: 10.1109/ACCESS.2022.3221400.
- [7] B. A. Tama, M. Comuzzi, and K.-H. Rhee, "TSE-IDS: a two-stage classifier ensemble for intelligent anomaly-based intrusion detection system," *IEEE Access*, vol. 7, pp. 94497–94507, 2019, doi: 10.1109/ACCESS.2019.2928048.
- [8] J. Jose and D. V Jose, "Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 1, pp. 1134–1141, Feb. 2023, doi: 10.11591/ijece.v13i1.pp1134-1141.
- [9] A. Boukhalfa, A. Abdellaoui, N. Hmina, and H. Chaoui, "LSTM deep learning method for network intrusion detection system," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp. 3315–3322, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3315-3322.
- [10] T. Nagaraj and R. K. Channarayappa, "An efficient security framework for intrusion detection and prevention in internet-of-things using machine learning technique," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 2, pp. 2313–2321, Apr. 2024, doi: 10.11591/ijece.v14i2.pp2313-2321.
- [11] B. Gao, B. Bu, W. Zhang, and X. Li, "An intrusion detection method based on machine learning and state observer for train-ground communication systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 6608–6620, Jul. 2022, doi: 10.1109/TITS.2021.3058553.
- [12] C. Zhou *et al.*, "Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 10, pp. 1345–1360, Oct. 2015, doi: 10.1109/TSMC.2015.2415763.
- [13] J. Zuniga-Mejia, R. Villalpando-Hernandez, C. Vargas-Rosales, and A. Spanias, "A linear systems perspective on intrusion detection for routing in reconfigurable wireless networks," *IEEE Access*, vol. 7, pp. 60486–60500, 2019, doi: 10.1109/ACCESS.2019.2915936.
- [14] X.-Y. Kong and G.-H. Yang, "An intrusion detection method based on self-generated coding technology for stealthy false data injection attacks in train-ground communication systems," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 8, pp. 8468–8476, Aug. 2023, doi: 10.1109/TIE.2022.3213899.
- [15] A. Sahu *et al.*, "Multi-source multi-domain data fusion for cyberattack detection in power systems," *IEEE Access*, vol. 9, pp. 119118–119138, 2021, doi: 10.1109/ACCESS.2021.3106873.
- [16] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, "HML-IDS: a hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," *IEEE Access*, vol. 7, pp. 89507–89521, 2019, doi: 10.1109/ACCESS.2019.2925838.
- [17] F. J. Mora-Gimeno, H. Mora-Mora, B. Volckaert, and A. Atrey, "Intrusion detection system based on integrated system calls graph and neural networks," *IEEE Access*, vol. 9, pp. 9822–9833, 2021, doi: 10.1109/ACCESS.2021.3049249.
- [18] J. Ning, J. Wang, J. Liu, and N. Kato, "Attacker identification and intrusion detection for in-vehicle networks," *IEEE Communications Letters*, vol. 23, no. 11, pp. 1927–1930, Nov. 2019, doi: 10.1109/LCOMM.2019.2937097.
- [19] C. Park, J. Lee, Y. Kim, J.-G. Park, H. Kim, and D. Hong, "An enhanced AI-based network intrusion detection system using generative adversarial networks," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2330–2345, Feb. 2023, doi: 10.1109/JIOT.2022.3211346.
- [20] P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, "An efficient intrusion prevention system for CAN: Hindering cyber-attacks with a low-cost platform," *IEEE Access*, vol. 9, pp. 166855–166869, 2021, doi: 10.1109/ACCESS.2021.3136147.
- [21] R. Ben Said, Z. Sabir, and I. Askerzade, "CNN-BiLSTM: a hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection," *IEEE Access*, vol. 11, pp. 138732–138747, 2023, doi: 10.1109/ACCESS.2023.3340142.
- [22] T. Kim and W. Pak, "Hybrid classification for high-speed and high-accuracy network intrusion detection system," *IEEE Access*, vol. 9, pp. 83806–83817, 2021, doi: 10.1109/ACCESS.2021.3087201.
- [23] J. Li, X. Tong, J. Liu, and L. Cheng, "An efficient federated learning system for network intrusion detection," *IEEE Systems Journal*, vol. 17, no. 2, pp. 2455–2464, Jun. 2023, doi: 10.1109/JSYST.2023.3236995.
- [24] M. Nadeem, A. Arshad, S. S. Band, and A. Mosavi, "Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system," *IEEE Access*, vol. 9, pp. 152300–152309, 2021, doi: 10.1109/ACCESS.2021.3126535.





- [25] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1594–1606, Sep. 2018, doi: 10.1109/TSMC.2017.2681698.

## BIOGRAPHIES OF AUTHORS







**Mangalapalli Vamsikrishna**     is currently working as a professor in the Department of IT, Aditya Engineering College (A), Surampalem, Kakinada. He has over 20+ years of teaching experience in various engineering colleges and universities. He pursued his MCA from IGNOU, followed by an M.Tech. in computer science from Sam Higginbottom University of Agriculture, Technology and Sciences (formerly Allahabad Agricultural Institute Deemed University) and subsequently completed another M.Tech. in artificial intelligence and robotics from Andhra University. He later earned his doctoral degree in medical image processing from Centurion University of Technology and Management. He has published over 90 articles in national and international journals and around 15 papers in national and international conferences. He has started guiding research scholars in areas such as cloud computing, medical image processing, data science, cyber security, and machine learning. To date, he has successfully guided 14 scholars who have been awarded doctoral degrees, and he is currently supervising 6 scholars. He can be contacted at email: [vkmgalampalli@gmail.com](mailto:vkmgalampalli@gmail.com).







**Garapati Swarna Latha**     is working as an associate professor in the Department of CSE, Rajamahendri Institute of Engineering and Technology, Rajamahendravaram. She completed her M.Tech. in CSE from GIET, affiliated with JNTUK Kakinada, in 2009. She has fourteen years of academic experience in various institutions. Before her M.Tech., she earned a bachelor of engineering in computer science and engineering from SVH College of Engineering, Machilipatnam (affiliated with Nagarjuna University) in 2002. Her interests include data mining, database management systems, cloud computing, and data structures. She has published many papers in national and international journals, guided various projects for B.Tech. students, conducted seminars and workshops, and visited various colleges for PG final year project adjudication. She can be contacted via email at [dasarwarnaprasad@gmail.com](mailto:dasarwarnaprasad@gmail.com).






**Gajjala Venkata Ramesh Babu**     is working as an associate professor in the Department of Computer Science at Sri Venkateswara University, Tirupati. He was awarded his Ph.D. in 2015 from Sri Venkateswara University, Tirupati. He pursued his M.Tech. from Vinayaka Mission University, Salem, and MCA from Osmania University, Hyderabad. He has 17 years of teaching experience in P.G. courses and 2 years in U.G. courses. He has published 70 research articles in different reputed journals and visited and presented 59 research papers at various national and international conferences in countries like China, Malaysia, and Singapore. His specializations include privacy-preserving data mining, cryptography and network security, software engineering, and applications of network security in e-commerce. He participated in 33 national workshops and seminars and organized 12 national workshops, seminars, and conferences. He is a member of three professional bodies and has served as deputy warden, NSS coordinator, and placement officer at Sri Venkateswara University. He has played an integral role as a special officer for examinations and professional courses at Sri Venkateswara University, Tirupati. He has been nominated as a BOS member for the Department of Computer Science at Sri Venkateswara University, Tirupati, Cluster University Kurnool, Duvvuru Ramanamma Degree and PG College, Gudur (Autonomous), Silver Jubilee Government College, Kurnool, and Vikrama Simhapuri University, Nellore, Andhra Pradesh. He can be contacted via email at [gvrameshbabu74@gmail.com](mailto:gvrameshbabu74@gmail.com).






**Koppiseti Giridhar**     is working as an assistant professor in the Department of Computer Science and Technology at Madanapalle Institute of Technology and Science. He has 12 years of teaching experience in various educational institutions across India. His expertise includes Java programming, machine learning, artificial intelligence, and various computer science courses. He has 8 years of research experience in wireless sensor networks, vehicular ad-hoc networks, and mobile ad-hoc networks. He is involved in research and project collaboration with other institutions and guides undergraduate students in real-time project implementations as well as research guidance. He can be contacted via email at [kgiridhar562@gmail.com](mailto:kgiridhar562@gmail.com).








**Lakshmeelavanya Alluri**    is currently, she is working as an assistant professor in the Department of CSE at SRKR Engineering College (A), located in Bhimavaram, Andhra Pradesh. She has 12 years of teaching experience. Her areas of interest include machine learning, deep learning, and IoT. She can be contacted at email: allurilavanya111@gmail.com.






**Giddaluru Somasekhar**    is currently working as an associate professor in the CSE Department at GITAM (Deemed to be University), Hyderabad. He has 14 years of teaching experience, with research areas including machine learning, data science, and big data analytics. He received his Ph.D. in big data analytics from VIT, Vellore, in 2019. He has published over 18 articles in reputed journals and presented 7 articles at international conferences, including 2 SCI-indexed and 10 SCOPUS-indexed papers. He has also participated in various workshops, faculty development programs, seminars, and training programs. He can be contacted via email at giddalurisomasekhar@gmail.com.



**Bhimunipadu Jestadi Job Karuna Sagar**    received his M.C.A. from J.N.T.U. College of Engineering Anantapuramu, Ananthapur, and his M.Tech. degree in computer science and engineering from Sathyabama University, Chennai. He earned his Ph.D. in wireless sensor networks from Dravidian University, Kuppam. Currently, he is a professor in the Computer Science and Engineering Department and has been the Dean of Faculty Affairs since 2022. With 21 years of teaching experience, he has supervised over 100 master's students and authored or co-authored more than 30 publications, along with several proceedings and journals with an H-index. His research interests include wireless sensor networks and hybrid routing protocols. He can be contacted at jksagar2003@yahoo.com.



**Naresh Dondapati**    received his B.Tech. and M.Tech. degrees from Jawaharlal Nehru Technical University-Kakinada, Kakinada, India. Currently, he is working as an assistant professor in the Department of ECE at Lakireddy Bali Reddy College of Engineering, Mylavaram. His areas of interest include analog and digital communications, image processing with LabVIEW, and machine learning. He can be contacted at email: naresh0475@gmail.com.