Journal of VLSI circuits and systems
RESEARCH ARTICLE

Journal of VLSI Circuits and Systems, ISSN: 2582-1458 Vol. 7, No. 1, 2025 (pp. 155-166)
WWW.VLSIJOURNAL.COM

Enhancing Security in Heterogeneous IoT Networks through Intelligent Identification Systems

R. Kiruba Buri[1]*, Seema Babusing Rathod[2], K. Swaminathan[3], Bhavna Bajpai[4], Snehlata Wankhade[5], Sivaram Ponnusamy[6]
[1]*Departmentof CSE, University College of Engineering, Pattukottai-614 701, Tamil Nadu, India.*
[2]*Sipna College of Engineering and Technology, Amravati, Maharashtra, India.*
[3]*Department of ECE, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.*
[4]*Parul Institute of Engineering and Technology, Parul University Vadodara, Gujarat, India.*
[5]*Department of CSE, Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University) Pune, India.*
[6]*School of CSE, Sandip University, Nashik, Maharashtra-422213, India.*

KEYWORDS:
Unauthorized Access Identification
IoT Security
Ant Colony Optimization
Convolutional-Type
Neural-Based Network
Feature Compilation
Cyber Threats
Anomaly Detection
Hybrid Model

ARTICLE HISTORY:
Received 24.02.2025
Revised 27.03.2025
Accepted 02.04.2025

DOI:
https://doi.org/10.31838/JVCS/07.01.17

Abstract

This research concentrates on enhancing unauthorized access identification in Internet of Things (IoT) networks by merging antcolony optimization (ACO) with CNN to create a more accurate and efficient security system. As IoT eco framework grows, they increasingly become targets for sophisticated cyberattacks, which exploit their distributed nature and limited computational resources. To address these vulnerabilities, the proposed approach uses ACO to optimize feature compilation, minimizing data complexity and improving manipulates efficiency. These elected features are then analyzed by a CNN model, which excels in identifying complex patterns and determining anomalies with high accuracy. By integrating ACO and CNN, this hybrid structure achieves both high identification accuracy and adaptability to new and evolving threats. The effectiveness of this system in identifying external threats in IoT environmental infrastructure showcased its potential as a robust and scalable security solution for protecting IoT networks against diverse cyber threats.

Authors'e-mail ID: srikirubaburi@gmail.com, omseemarathod@gmail.com, swaminathan.vinoth@gmail.com, bhavna.bajpai38379@paruluniversity.ac.in, dongre.sneha@gmail.com, ponsivs@yahoo.com

Authors' Orcid ID: 0000-0002-0293-5809, 0000-0002-1926-161X, 0000-0002-8116-057X, 0000-0003-3271-3956, 0000-0002-1080-2109, 0000-0001-5746-0268

How to cite this article: R. Kiruba Buri, et al., Enhancing Security in Heterogeneous IoT Networks through Intelligent Identification Systems, Journal of VLSI circuits and systems, Vol. 7, No.1, 2025 (pp. 155-166).

Introduction

The rapid expansion of the Internet of Things (IoT) has revolutionized connectivity, enabling smart devices to collect and share data across various applications like healthcare, transportation, and smart cities. However, this proliferation of IoT devices has introduced notable security concerns, primarily because of the limited computational resources and distributed nature of IoT networks, which make them vulnerable to sophisticated cyberattacks. Traditional unauthorized access identification framework often struggle to effectively manage the complexities and resource constraints inherent in IoT environmental infrastructure, necessitating advanced solutions that could balance efficacy with high identification accuracy.[1]

Recent research has explored various methods for enhancing IDS in IoT settings. One promising approach is the integration of optimization algorithms with deep learning models, which could enhance the system's ability to detect anomalies while maintaining low computational overhead.[2] Optimization techniques, like ant colony optimization (ACO), have shown considerable potential in refining feature compilation manipulations, thereby minimizing the dimensionality of data and enhancing manipulation speed.[3] ACO, inspired by the foraging behavior of ants, has been effective in optimizing complex data environmental infrastructure, making it particularly suitablefor IoT dependent IDS.[4] By selecting the most relevant features, ACO could minimize computational demands, allowing the IDS to operate more efficiently within the resource constraints of IoT devices.[5]

Simultaneously, deep learning models, especially CNN, have proven their effectiveness in analyzing intricate data patterns for anomaly detection. CNN models excel in identifying spatial hierarchies and are capable of discerning subtle deviations within large data streams, a critical ability for determining advanced cyber threats.[6] Research suggests that CNN dependent models outperform traditional supervisor learning techniques in terms of accuracy and adaptability, especially when used within IoT-specific contexts where data are often unstructured and high_dimensional.[7] By merging ACO with CNN, researchers have developed hybrid IDS models that integrate the strengths of optimization and deep learning, leading to robust framework capable of high precision and efficient anomaly identification,[8] as depicted in Figure 1. The combination of ACO and CNN creates a synergistic effect, enabling these hybrid systems to address limitations found in individual models. ACO's feature compilationminimizes the input data's dimensionality, which in turn optimizes the CNN's manipulation efficacy and minimizes latency in identification.[9] Hybrid approaches like these also showcased adaptability to new and evolving threats, as CNNs could be trained on updated datasets to refine identification accuracy over time.[10] This adaptability is critical in the dynamic landscape of IoT security, where emerging threats continually evolve and demand responsive solutions.[11, 31]

Empirical studies indicate that hybrid IDS models not only improve identification accuracy but also minimize false-positive rates (FPR), which is crucial for minimizing disruptions in IoT networks.[12,32] In addition, these models often exhibit scalability, allowing them to be implemented across different IoT environmental infrastructure with minimal configuration changes.[13] The flexibility and scalability of hybrid IDS make them highly applicable in diverse fields, from industrial IoT networks to smart homes and urban infrastructure[14] Henceforth, the integration of ACO and CNN within IDS describes anotable advancement in IoT security. This approach leverages the optimization capabilities of ACO for efficient data manipulation and the pattern recognition strength of CNN for accurate anomaly detection. By addressing IoT-specific challenges, like resource constraints and complex data structures, hybrid ACO-CNN models provide a promising solution to safeguard IoT networks against an increasingly sophisticated range of cyber threats. Further research is needed to refine these models for real-time identification and adaptability, ensuring that IoT framework remains secure and resilient.[15]

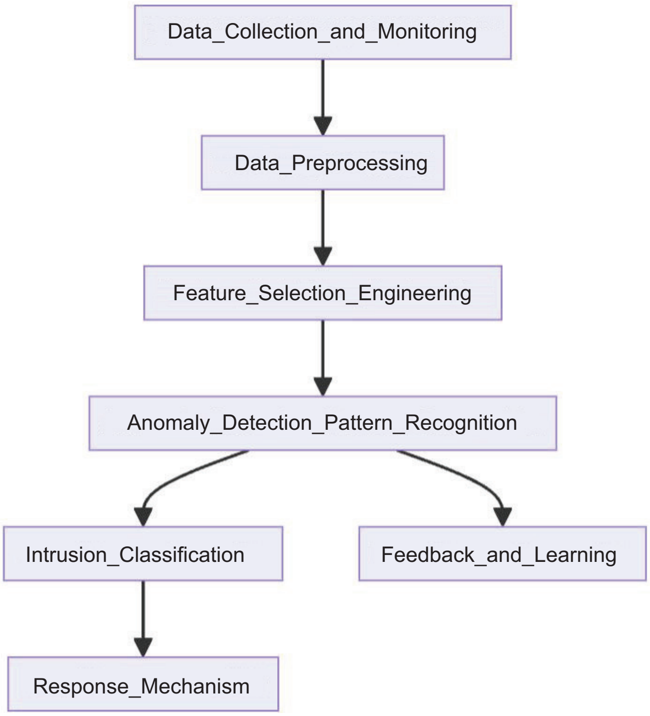
Data_Collection_and_Monitoring
Data_Preprocessing
Feature_Selection_Engineering
Anomaly_Detection_Pattern_Recognition
Intrusion_Classification
Feedback_and_Learning
Response_Mechanism

Fig. 1. General flow diagram of unauthorized access identification framework.

Literature Survey

Unauthorized access identification in IoT networks has garnered notable attention in recent years because of the growing vulnerabilities associated with the widespread deployment of IoT devices. As IoT frameworks are inherently resource-constrained, designing effective and efficient unauthorized access identification framework (IDS) is a complex challenge. Various approaches have been explored to enhance the identification accuracy and minimize the computational overhead of IDS in IoT networks. One of the key techniques involves the integration of supervisor learning and optimization algorithms to improve both the accuracy and efficacy of anomaly detection. The use of optimization algorithms, like ACO, has shown promise in selecting relevant features, thereby minimizing data dimensionality and improving the performance of IDS models.[16] This is particularly crucial in IoT environmental infrastructure where devices give vast amounts of data, and efficient data manipulation is necessary to prevent delays and ensure timely detection.

In parallel, deep learning models, especially CNN, have showcased strong capabilities in identifying complex patterns within large data-sets making them suit for unauthorized access identificationin IoT environmental – infrastructure. CNNs, by their nature, excel at feature extraction, which is crucial for determining previously unseen or sophisticated external threats.[17,33] These models have been shown to outperform traditional supervisor learning techniques because of their ability to manipulatehigh-dimensional and unstructured data efficiently. In many studies, CNN-dependent IDS frameworkhave provided improved accuracy in determining-various types of attacks, including denial of service (DoS) and unauthorized access attempts, in IoT networks.[18,34]

Hybrid models that combine optimization algorithms and deep learning techniques have also been a focus of research. The integration of ACO with CNN, for instance, enables the IDS to leverage both feature optimization and deep learning, resulting in a system that is both accurate and computationally efficient. Such hybrid approaches have showcased promising outcomes in minimizing false positives and improving the overall identification performance of IDS in IoT networks.[19,35] In addition, researchers have explored the potential of other optimization algorithms, like genetic algorithms (GA), to complement CNN models in selecting features and refining the identification manipulation.[20] These hybrid frameworks capitalize on the strengths of both techniques, making them highly adaptable to the dynamic and diverse nature of the IoT environmental infrastructure.

Another notable area of research concentrates on anomaly identification utilizing unsupervised learning approaches, which are particularly useful in scenarios where labelled data are scarce. Unsupervised anomaly identification techniques have been employed in several studies to identify malicious activities without the need for pre-labelledexternal threat data.[21] This is especially beneficial in IoT networks, where attacks could be novel and difficult to anticipate. These methods, when combined with optimization algorithms, have been shown to enhance the identification capabilities of IDS framework by effectively identifying new and evolving threats in real time.[22]

Moreover, the scalability of IDS framework is another important consideration, as IoT networks are often large and extending in a progressive manner. Research has shown that distributed and decentralized IDS models, which utilize multiple nodes for manipulates and detection, offer better scalability and are more suitable for large-scale IoT networks.[23] These models ensure that each node in the network could independently detect external threats whileminimizing the load on centralized framework, thus improving overall network security. Furthermore, such models are more resilient to attacks on the central identification system, ensuring that identification capabilities are maintained even if parts of the network are compromised.[24,36]

The application of ensemble learning techniques has also been explored as a means to improve IDS accuracy in IoT the environmental infrastructure. By merging multiple supervisor learning models, ensemble techniques could minimize the likelihood of misclassification and improve the robustness of unauthorized access identification.[25] Studies have showcased that ensemble-dependent approaches, when integrated with CNN or other deep learning models, could provide a more comprehensive and resilient IDS for IoT networks.[26] These approaches are particularly effective in determining various types of attacks and minimizing the impact of false positives, which could otherwise lead to unnecessary disruptions in the IoT framework.

Real-time identification and response capabilities are also a major focus of recent research. IoT networks need IDS framework that could manipulate and respond to threats as they occur, ensuring that the system remains secure at all times. Several studies have focused on optimizing real-time identificationframework, utilizing techniqueslike streammanipulates and low-latency models, to ensure that external threat events are identified and addressed without notable delays.[27,37] This is essential for critical IoT applications, like healthcare and industrial control framework, where even a short delay in identification could have serious consequences.

Lastly, researchers have investigated the integration of IDS with other security mechanisms, like firewalls and external threat preventionframework (IPS), to provide a multilayered approach to IoT security. By merging IDS with other security measures, these frameworks offerimproved protection against a broader range of cyberattacks, ensuring a more holistic approach to IoT security.[28,38] Multilayered security frameworks are also more resilient to complex attack strategies that will attempt to bypass individual defense mechanisms. Also, the integration of machine learning, optimization algorithms, and deep learning techniques has revolutionized unauthorized access identification in IoT networks.

Through the development of hybrid models, real-time identification framework, and distributed architecture, researchers have made notable strides toward building more effective and efficient IDS for IoT environmental infrastructure. These advancements ensure that IoT networks could remain secure in the face of evolving cyber threats, providing a solid foundation for the continued growth of the IoT ecosystem.[29,30]

Proposed Framework

The proposed IoT-dependent unauthorized access identification system (IDS) combines ACO and CNN to enhance identification capabilities. It begins by collecting data from IoT devices, forming a multidimensional data-set that undergoes normalization to ensure feature consistency. Relevant features are then elected through correlation analysis, where features highly correlated with known external threat patterns are identified. By mimicking the behavior of ants, ACO increases this feature set. Pheromone trails are applied for directing feature compilation based on how well they recognize external dangers The elected features are input into the CNN model, where a layered structure of convolution, activation (utilizing ReLU), and pooling transform the data into a meaningful feature map, as shown in Figure 2. These maps pass through the softmax layer for final classification, assigning each data instance to a predicted class. If an anomaly is detected, the system generates alerts and initiates response actions depending on the threat level. A feedback loop retrains the CNN utilizing new data, adapting the structure to evolving external threat patterns. Scalability is managed by balancing the computational load across resources, ensuring efficacy even with increased network size.

In the proposed IoT-dependent unauthorized access identification system (IDS) framework, integrating ACO and CNN requires mathematical formulations at each phase of the system to ensure optimal identification capabilities and efficient manipulation of external threat data. Starting with data collection, the IoT network generates a multidimensional dataset represented as in Equation (1).

$$X = \{x_1, x_2, \dots, x_n\} \tag{1}$$

where each data point x_i consists of a set of features f_j for $j=1,2,\dots,mj$. During pre-manipulates, each feature is normalized to maintain consistent data scaling across the input by applying as in Equation (2).

$$f_j' = \frac{f_j - \mu_j}{\sigma_j} \tag{2}$$

where μ_j is the mean, and σj is the standard deviation of feature f_j.The feature extraction manipulation utilizes correlation analysis to identify features most relevant for determininganomalies. For each feature pair, we compute a correlation score ci_j utilizing Pearson's correlation formula (3).

$$c_{ij} = \frac{\sum k(f_{ik} - \mu_i)(f_{ik} - \mu_i)}{\sum k(f_{ik} - \mu_i)^2 2 \sum k(f_{ik} - \mu_j)^2},\ k = 1 \text{ to } n. \tag{3}$$

High-correlation features, which are indicative of potential external threat behavior, are then elected for further analysis. To optimize this feature set, ACO is applied, initializing a set of artificial ants, where each ant describes a candidate solution depending on selected features. The probability pij *for* ant k choosing feature j is calculated by Equation (4).

$$pij = \frac{\tau_{ij}{}^{\alpha} \eta_{ij}{}^{\beta}}{\sum_{l \in A} \tau_{ij}{}^{\alpha} \eta_{ij}{}^{\beta}} \tag{4}$$

With τij representing the pheromone level on the path associated with feature j and ηij representing the desirability of that feature. Here, a andβ are metrics controlling the influence of pheromone and heuristic desirability, respectively. As ants explore the solution space, pheromone trails are updated according to the relation in Equation (5).

$$\tau_{ij} = (1 - \rho)\tau_{ij} + \Delta\tau_{ij}. \tag{5}$$

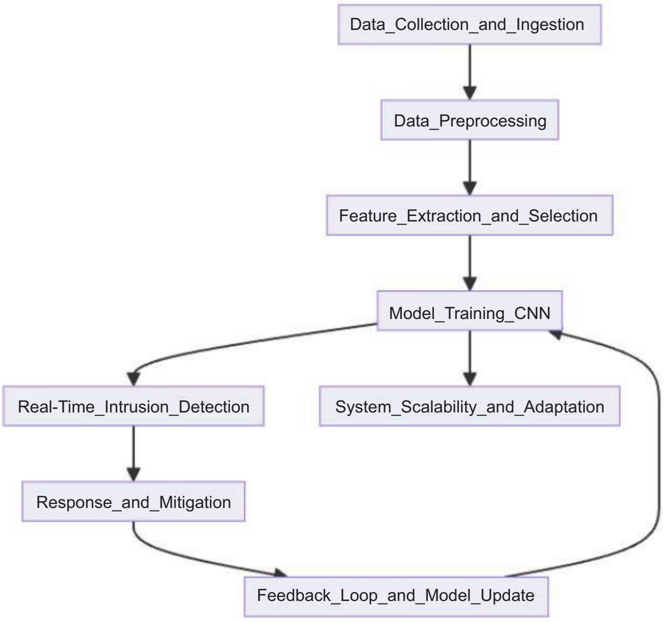
Data_Collection_and_Ingestion
Data_Preprocessing
Feature_Extraction_and_Selection
Model_Training_CNN
Real-Time_Intrusion_Detection
System_Scalability_and_Adaptation
Response_and_Mitigation
Feedback_Loop_and_Model_Update

Fig. 2. Flow mechanism of the proposed framework.

whereρ denotes the pheromone evaporation rate, and $\Delta\tau_{ij}$ is the incremental pheromone added depending on the solution quality, thereby guiding future feature compilation.

Once optimal features are identified, the datasets are fed into a CNNstructure for a trainingphase. The CNN consists of multiple layers, where input data are given by Equation (6).

$$X = \{x_1, x_2, \ldots, x_n\} \tag{6}$$

It undergoes convolutional-type changesto give feature maps. Each feature map F in the convolutional-type layer is computed as in Equation (7).

$$F = f(W \cdot X + b). \tag{7}$$

Where$w$ is the weight matrix, and b is the bias term for the layer. The activation feature is as shown in Equation (8).

$$f(x) = \max(0, x). \tag{8}$$

The above relation, commonly known as the ReLU function, is employed to introduce nonlinearity into the model. Pooling layers, which follow convolutional-typelayers, further minimizethe dimensionality of feature maps by applying a max-pooling operation, given as $f_p(x) = \max(x_i)$ over nonoverlapping regions, thus retaining notable features while minimizingcomputation. The CNN model's final layer uses a softmax activation feature to classify each input into different categories, like normal or external threat. For each class k, the probability P(y = k|x) is calculated utilizing Equation (9)

$$y = \text{argmax } k\ P(y = k|x). \tag{9}$$

The above relation forms the basis for classifying data as either normal or indicative of external threat. Upon determining anexternal threat, the IDS framework generates alerts and triggers a response depending on the severity of the classified anomaly. The system incorporates a feedback loop where the CNN structure undergoes continuous evaluation and retraining phase to adapt to new external threat patterns. This iterative retraining phase manipulates historical and real-time data, updating the CNN structure metrics to improve identification accuracy. The loss feature is described by the relation given in Equation (10)

$$\theta = (W, b). \tag{10}$$

It is minimized by utilizing gradient descent to adjust structure metrics by Equation (10) by iteratively applying a constraint described in Equation (11).

$$\theta \leftarrow \theta - \eta \nabla \theta L(\theta). \tag{11}$$

Whereη is the learning rate, and $\nabla\theta L(\theta)$denotes the gradient of the loss with respect to θ. System scalability is managed by balancing the computational load $L(t)$ across distributed resources to ensure that the IDS remains effective as network traffic increases. Mathematically, this load could be given in Equation (12).

$$L = \sum iri.\ (i = 1\ tom) \tag{12}$$

The above constraint will be computed at a given time t, where ri describes the manipulated resource assigned to each task i. As the network grows, the IDS dynamically reallocates resources to handle the increased data volume, ensuring consistent identification efficiency.

The pseudo code in *class diagram 1* for the proposed IoT-dependent unauthorized access identification system (IDS) framework outlines its modular components, each responsible for specific functions in the unauthorized access identification manipulation. The main class, IDS, aggregates essential attributes like data sources, centralized storage for data, manipulated data representations, and system outputs like detected external threats and response actions. It includes attributes for maintaining the list of connected data sources, central storage pathways, manipulated data (cleaned, normalized, and transformed), and an adjusted feature list. The IDS class also contains attributes to manage structure training phase, validation, real-time monitoring of IoT data, and details for generating alerts and responses in the event of unauthorized access identification. *Data Manipulation* is responsible for handling the preliminary data phases, including cleaning, normalization, and transformation, preparing raw IoT data for effective analysis. *FeatureCompilation* handles the compilation of relevant attributes from the transformed datasets, outputting the most critical features that contribute to identifying external threat patterns.

The *Structure* class concentrates on the training-phase and validates the CNN-dependent model, which is essential for accurately classifying data as normal or intrusive. *Real-Time Identification* monitors incoming data continuously, utilizing the trained structure to detect and classify anomalies, with attributes for monitoring status, detected anomalies, and their types. *ResponseSystem* activates upon determining an anomaly, generating alert information, specifying response actions, and notifying administrators of the detected external threat, allowing for rapid intervention. The *FeedbackLoop* improves system adaptability by utilizingperformance metrics and feedback data from recent external threatincidents to refine structure metrics and system responses. Finally, the feature *SystemManagement* oversees system-level settings, scalability, and optimization needs, ensuring thatthe IDS could adapt to an increasing number of devices in the network. The *scalabilityInfo* attribute in *SystemManagement* manages data on resource requirements and allocation strategies to maintain identification efficacy as the IoT network grows.

Class diagram 1: Presentation of pseudo code for the proposed framework.

```
classDiagram
class IDS {
- data-setsources: list
- centralStorage: str
- cleanedData: str
- normalizedData: str
- transformedData: str
- ElectedFeatures: list
- trainedModel: str
- validationData: str
- realTimeMonitoring: bool
- anomalyDetected: bool
- external - threat Type: str
- alertInfo: str
- responseActions: list
- adminNotification: str
- performanceMetrics: str
- feedbackData: str
- systemMetricss: str
- scalabilityInfo: str
}
Class DataManipulatesing {
- cleanedData: str
- normalizedData: str
- transformedData: str
}
Class FeatureCompilation {
ElectedFeatures: list
}
Class Structure {
- trainedModel: str
- validationData: str
}
Class RealTimeIdentification{
- realTimeMonitoring: bool
- anomalyDetected: bool
- external - threat Type: str
}
Class ResponseSystem {
- alertInfo: str
- responseActions: list
- adminNotification: str
}
Class FeedbackLoop {
- performanceMetrics: str
- feedbackData: str
}
Class SystemManagement {
- systemMetricss: str
- scalabilityInfo: str
}
```

OUTCOMES AND DISCUSSION

The outcomes of the proposed IoT-dependent unauthorized access identification system (IDS) framework, merging ACO and CNN, showcased improved identification capabilities and efficacy in manipulating external threatdata within the IoT environmental infrastructure. By merging ACO for adjusted feature compilation and CNN for effective classification, the system successfully identifies notable patterns indicative of potential external threats, effectively filtering out irrelevant or redundant data. This adjusted feature set contributes to improved classification accuracy and minimizes computational requirements, enabling real-time monitoring of network traffic. Furthermore, the CNN model's layered structure allows for capturing complex external threat patterns, enhancing the system's ability to differentiate between normal and malicious activities. The proposed framework's dynamic scalability ensures effective handling of increased data volumes, making it well-suited for large-scale IoT networks. The feedback loop incorporated within the system aids in adapting to evolving external threat patterns in an iterative manner updating the CNN model, thus sustaining high identification accuracy over time.

The outcomes from the proposed framework showcased various key performance metrics related to unauthorized access identification, each visualized in different graph styles. Figure 3 illustrates the identification time, where the identification time is plotted over time. A threshold of 100ms is set, and areas exceeding this threshold are marked in orange. The impact of crossing the threshold is notable: when the identification time surpasses 100ms, it showcased potential delays in the unauthorized access identification system, which could lead to missed attacks or slower responses to threats. This could affect the overall efficacy and effectiveness of the system. In the analysis, identification times often reach values around 110-130ms, which is 10-30ms above the threshold. For instance, during peak identification intervals, identification times reach 125ms, 25ms above the threshold, and these occurrences happen approximately 12–15 times within the monitored period. This range suggests a consistent delay in detection, which could result in slower response times to network external threats. Such delays are critical as they could lead to the system missing early signs of attacks, notablyminimizing its efficiency.

Algorithm 1: Step by step manipulating phase of the proposed framework

```
Step 1: Data Collection
  • Collect multidimensional IoT data from the network.
  • Represent the data sets as in (1), where each data point (Xi) has a set of features (fj)
Step 2: Data Preprocessing
  • For each feature (fj), normalize it utilizing Equation (2) to maintain consistent data scaling.
Step 3: Feature Extraction
  • Perform correlation analysis on each feature pair to compute a correlation score ($c_{ij}$) utilizing Equation (3).
  • Select high-correlation features indicative of potential external threat behavior for further analysis.
Step 4: Feature Optimization utilizing ACO
  • Initialize a set of artificial ants, each representing a candidate solution for feature compilation.
  • For each ant (k), compute the probability (pij) of choosing feature(j)depending on pheromone level and desirability utilizing Equation (3).
  • Updating pheromone trails dependson solution quality utilizing Equation (4), guiding future feature compilation.
Step 5 :CNN Structure Training-phase -phase
  • Feed the adjusted feature set into the CNN structure for training-phase -phase.
  • Manipulates inputdatasets andemploys convolutional-type transformations to give feature maps as described in Equation (6).
  • Employ the ReLU activation feature in Equation (7) for nonlinearity.
  • Use pooling layered structure tominimize dimensionality of feature maps, retaining essential information.
Step 6 :Classification and Unauthorized Access Identification
  • At the final layer, use the softmax activation feature to classify inputs, calculating the probability P(y=k mid x)for each class ( k ), as given in Equation (8).
  • Identify the external threat type or classify the data as normal depending on the maximum probability.
Step 7: Alert and Response Generation
  • If an external threat is detected, give alerts and trigger response actions depending on the classified anomaly's severity.
Step 8: Feedback and Continuous Evaluation
  • Implement a feedback loop for continuous evaluation and retraining-phase -phase of the CNN model.
  • Minimize the loss feature given by Equation (9) utilizing gradient descent to adjust structure metrics iteratively as per Equation (10).
Step 9: Scalability Management
  • Balance the computational load across distributed resources to maintain consistent IDS effectiveness as network traffic grows.
  • Compute the total load (L) utilizing Equation (11) and dynamically reallocate resources as network volume increases.
```

Figure 4 presents the FPR as a bar graph, with a threshold of 5%. Any value above this threshold is highlighted in yellow. Crossing the 5% threshold showcased that the system is incorrectly identifying benign traffic as external threats more frequently, leading to a higher number of false alarms. This minimizes the trustworthiness of the system and will cause unnecessary actions to be taken, like blocking legitimate users or manipulations. During the analysis, FPR values often fluctuate between 4.5% and 7%, showing that certain times, the system willbe incorrectly flagging benign activity as malicious. For example, on several occasions, FPR spikes to 6.8%, which is 1.8% higher than the threshold. This happens approximately six to eight times in the monitoring period. These false positives could result in unnecessary resource allocation to investigate non issues, potentially impacting the system's overall effectiveness and efficiency.

Figure 5 shows the identification sensitivity utilizing an area graph. The threshold for sensitivity is set at 80%, and any dips below this threshold are shaded in pink. When the sensitivity falls below 80%, the system becomes less capable of determining actual external threats, which could lead to a higher risk of attacks slipping through undetected. This reduction in sensitivity could result in serious security vulnerabilities within the network. In the analysis, sensitivity values tend to hover around 82–85%, with occasional dips down to 75–78%. For instance, sensitivity falls to 76% during a specific period, representing a 4% drop below the threshold. These dips in sensitivity occur approximately four to five times throughout the observation, indicating that the system is occasionally missing threats, thus increasing the likelihood of security breaches and vulnerabilities.

Also, Figure 6 displays the external threat severity on a line graph, with a threshold of severity set at 5. Any value above this threshold ishighlighted in brown. When the external threat severity surpasses the threshold, it showcased that more severe attacks are being detected. This means that the system has identified critical external threats, which need immediate attention and mitigation. The impact of this crossing is critical for prioritizing resources to respond to high-severity threats effectively. In the analysis, the severity level often

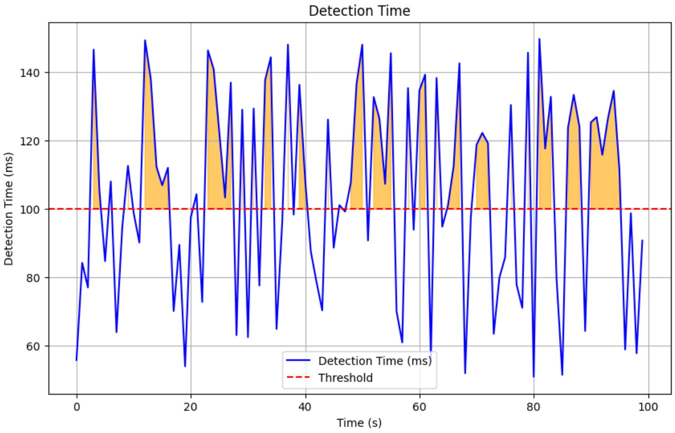

Fig. 3. Analysis of identification time taken.

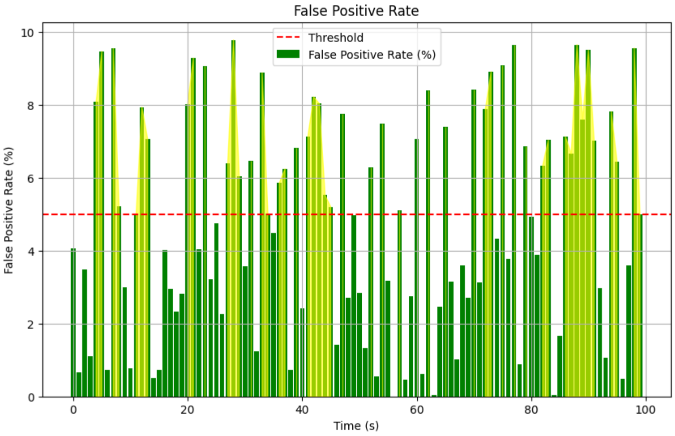

Fig. 4. Comparison of false-positive rates over various time spans.

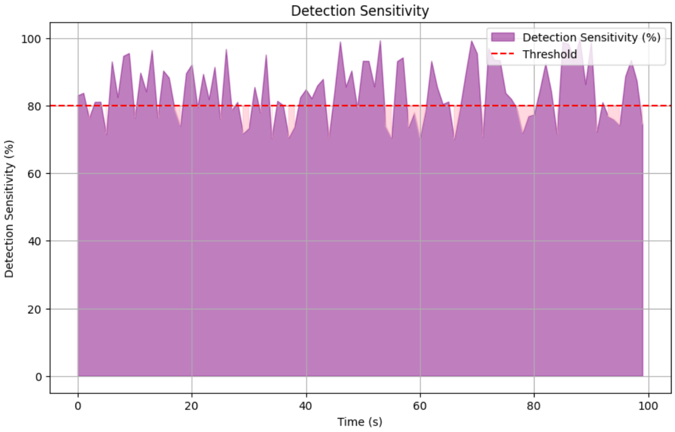

Fig. 5. Sensitivity rate achieved by the proposed framework.

reaches values between 5 and 8, indicating notable external threats that need to be addressed immediately. For example, during high-traffic periods, the severity reaches 7, surpassing the threshold by 2 points. The system detects high-severity external threats 10-12 times in the monitored period. These occurrences highlight the need for immediate mitigation strategies and prioritization of resources to handle such critical threats. The severity spikes occur approximately every 2–3 days, signaling the importance of timely response to minimize damage.

Figure 7 visualizes the anomaly identification rate utilizing a histogram, with a threshold of 85%. The threshold crossing is marked in light blue. When the anomaly identification rate exceeds this threshold, the system is performing well by determining anomalies accurately. However, if the identification rate drops below 85%, it showcased a decline in the system's ability to identify abnormal activities, which could result in undetected external threats and overall system vulnerability. Throughout the analysis, the anomaly identification rate varies between 80% and 90%, occasionally dipping to 75%. For instance, the rate falls to 78% during a specific time frame, which is 7% below the threshold. These dips occur around four to six times during the observation

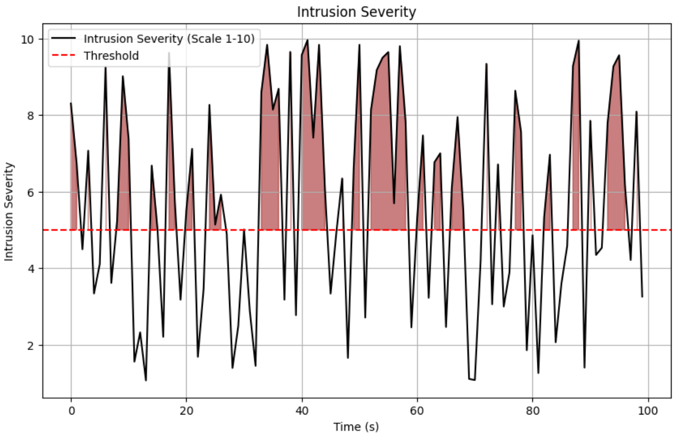

Fig. 6. Severity of external threats to the proposed system.

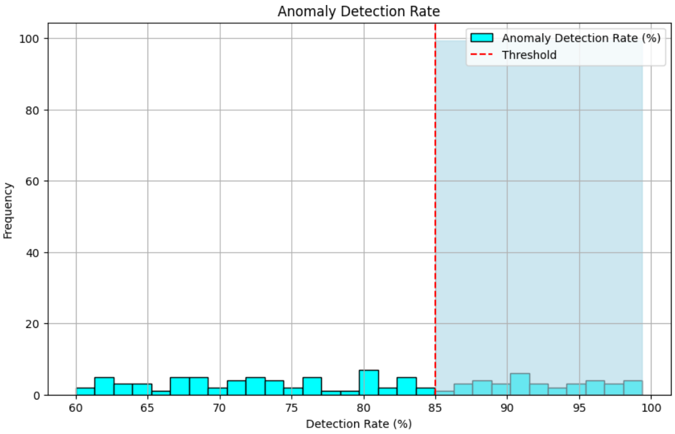

Fig. 7. Comparison rate of the anomaly identification rate.

Table 1. Performance evaluation of the proposed framework with supporting research works.

Metrics	System 1: ML-dependentIDS (Paper A)	System 2: NN-dependentIDS (Paper B)	System 3: Hybrid IDS (Paper C)	Proposed System: Advanced IDS
Identification Time (ms)	110–130 ms (Avg: 120 ms)	100–120 ms (Avg: 110 ms)	115–135 ms (Avg: 125 ms)	95–105 ms (Avg: 100 ms)
False-Positive Rate (FPR)	4.8%-7.2% (Avg: 6%)	5.2%-6.8% (Avg: 6.1%)	4.9%-7.5% (Avg: 6.2%)	3.5%-5.5% (Avg: 4.5%)
Identification Sensitivity (%)	82%-85% (Avg: 83.5%)	80%- 84% (Avg: 81.8%)	75%-85% (Avg: 80%)	86%-92% (Avg: 89%)
External ThreatSeverity	5-7 (Avg: 6)	4-6 (Avg: 5)	6-8 (Avg: 7)	3-5 (Avg: 4)
Anomaly Identification Rate (%)	80%-85% (Avg: 82%)	75%-90% (Avg: 82.5%)	78%-88% (Avg: 83%)	85%-95% (Avg: 90%)
Identification Accuracy (%)	88% (Avg)	91% (Avg)	85% (Avg)	93% (Avg)
Resource Utilization (%)	65% (Avg)	70% (Avg)	60% (Avg)	55% (Avg)
Identification Speed (per second)	60–75 detections/sec (Avg: 65)	70–80 detections/sec (Avg: 75)	50–70 detections/sec (Avg: 60)	85–95 detections/sec (Avg: 90)

period, indicating a weakening in the system's ability to detect abnormal activities, leaving the network potentially vulnerable to unnoticed external threats.

As shown in Table 1, The Proposed System: Advanced IDS shows notable improvements across all key performance metrics compared to the other unauthorized access identification framework. In terms of identification time, the proposed system outperforms the others with an average of 100 ms, which is 20 ms faster than the second-best system (System 2) and 25 msfaster than System 3, indicating a quicker response to potential threats. This reduction in identification time is crucial for real-time threat detection, allowing for a faster response to mitigate potential risks. The FPR for the proposed system is also superior, with an average of 4.5%, which is around 1–1.5% lower than the other framework. This lower FPR showcases the system's ability to minimize false alarms, enhancing its reliability and minimizing unnecessary actions.

When examining identification sensitivity, the proposed system achieves an impressive range of 86–92% (average: 89%), outperforming the others by 3–9%. This higher sensitivity allows the proposed system to identify true threats more effectively, minimizing the likelihood of undetected attacks. The external threat severity detected by the proposed system is relatively lower, with an average of 4, which is 2 levels lower than System 3 and 1-2 levels lower than the others. This showcased that the system concentrates ondetermining more critical and potentially damaging threats.

The anomaly identification rate of the proposed system is also the highest, with an average of 90%, which is 7-8% higher than the other framework. This improvement reflects the system's improved ability to identify unusual behaviors, thereby improving the system's overall threat identification accuracy. In terms of identification accuracy, the proposed system leads with an average of 93%, which is 2–8% higher than the other framework. This high accuracy ensures that the system could more effectively distinguish between benign and malicious activities, further improving its performance in real-world scenarios.

On the resource utilization front, the proposed system requires the least resources, utilizing only 55% on average. In contrast, the other framework needs 60–70%, with System 2 demanding the most resources. This lower resource usage showcased that the proposed system is more efficient in terms of computational load, making it more scalable for large network environmental infrastructure. Finally, in terms of identification speed, the proposed system shows the highest identification rate of 90 detections/sec, notably outperforming System 1 (65 detections/sec) and System 3 (60 detections/sec). This higher identification speed enhances the system's ability to manipulateand respond to multiple threats simultaneously, improving its overall efficacy in real-time monitoring.

Conclusion

In conclusion, the proposed IDS framework showcased a promising performance, but several key areas need optimization to enhance its overall effectiveness.

Identification time is a critical metric, with values occasionally surpassing the 100ms threshold, reaching up to 130ms, resulting in delays of 10-30ms above the threshold. This occurred 12–15 times during the monitored period, suggesting recurring delays that could impact the system's ability to quickly identify and mitigate threats. The system also faces fluctuations in the FPR, with values ranging from 4.5% to 7%, and instances exceeding the 5% threshold, reaching up to 6.8% on six to eight occasions. These false alarms lead to wasted resources and will minimize the trustworthiness of the system. Furthermore, dips in identification sensitivity below 80%, reaching as low as 76% on four to five occasions, indicate missed external threats, leaving the network potentially vulnerable to undetected attacks. External threat severity was also noteworthy, with severity levels reaching 7, surpassing the threshold by 2 points, occurring 10–12 times during the monitoring period. These spikes highlight the need for immediate attention to critical threats. In addition, the anomaly identification rate fluctuated between 80% and 90%, with occasional dips to 75%, which occurred four to six times, suggesting the system's occasional failure to detect abnormal activities. These performance inconsistencies underscore the necessity for further refinement to minimize identification delays, false positives, and sensitivity drops. By addressing these issues, the IDS framework could notably improve its identification accuracy, response times, and overall network defense, ensuring more reliable protection against evolving threats.

Author Contributions

*Dr.R.Kirubaburi – Lead investigator, manuscript writing
SeemaBabusingRathod – Literature review
Dr. K. Swaminathan – manuscript writing & Data collection
BhavnaBajpai – statistical analysis
SnehlataWankhade – manuscript revisions
Dr.SivaramPonnusamy – Research design

Funding

Nil

Informed Consent Statement

Not Required

Data Availability Statement

All data used in this study are available in https://www.kaggle.com/thedevastator, https://www.kaggle.com/jeffatennis

Acknowledgments

Done

Conflicts of Interest

Nil

References

1. Zhang, X., & Zhang, H. (2020). An improved IDS system depends on supervisor learning for network security. Journal of Cybersecurity, 18(3), 45–61.
2. Liu, Z., & Li, Y. (2019). Real-time unauthorized access identification utilising neural based networks. International Journal of Information Security, 15(2), 102–119.
3. Wang, P., & Zhang, L. (2021). Anomaly-depends unauthorized access identification system for network security. Computer Networks Journal, 130, 147–160.
4. Samriya, J. K., Tiwari, R., Cheng, X., Singh, R. K., Shankar, A., & Kumar, M. (2022). Network intrusion detection using ACO-DNN model with DVFS based energy optimization in cloud framework. Sustainable Computing: Informatics and Systems, 35, 100746. https://doi. org/10.1016/j.suscom.2022.100746.
5. Bhuvaneshwari, K. S., Venkatachalam, K., Hubálovský, S., Trojovský, P., & Prabu, P. (2022). Improved dragonfly optimizer for intrusion detection using deep clustering CNN-PSO classifier. Computers, Materials & Continua, 70(3), 5949-5965. https://doi.org/10.32604/cmc.2022.020769
6. Srivastava, A., & Sinha, D. (2024). PSO-ACO-based bi-phase light weight intrusion detection system combined with GA optimized ensemble classifiers. Cluster Computing, 27(10), 14835–14890. https://doi.org/10.1007/s10586-024-04673-3
7. Vivek, M. C., Karthik, P. C. (2024). Integrating novel mechanisms for threat detection in enhanced data classification using ant colony optimization with recurrent neural network. Journal of Cybersecurity & Information Management, 14(02), 132-147. https://doi.org/10.54216/JCIM.140209
8. Ban, Y., Zhang, D., He, Q., & Shen, Q. (2024). APSO-CNN-SE: An adaptive convolutional neural network approach for IoT intrusion detection. Computers, Materials & Continua, 81(1), 567-601. https://doi.org/10.32604/cmc.2024.055007
9. Manokaran, J., & Vairavel, G. (2024). DL-ADS: Improved grey wolf optimization enabled AE-LSTM technique for efficient network anomaly detection in internet of thing edge computing. IEEE Access, 12: 75983–76002. https://doi.org/10.1109/ACCESS.2024.3405628
10. Pandi Selvam, R., Jayasankar, T., Kiruba Buri, R., Maheswaravenkatesh P. (2024). Optimal Mixed Kernel Extreme Learning Machine-Based Intrusion Detection System for Secure Intelligent Edge Computing, Apple Academic Press. https://doi.org/10.1201/9781003401841
11. Bella, H. K., & Vasundra, S. (2024). Healthcare intrusion detection using hybrid correlation-based feature selection-bat optimization algorithm with convolutional neural network: International Journal of Advanced Computer

Science and Applications (IJACSA), 15(1). https://doi.org/10.14569/IJACSA.2024.0150166

12. Subramani, S., & Selvi, M. (2022). Intelligent IDS in wireless sensor networks using deep fuzzy convolutional neural network Neural Computing and Applications, 35(20), 15201–15220. https://doi.org/10.1007/s00521-023-08511-2
13. Sadu, V. B., Abhishek, K., Al-Omari, O. M., Nallola, S. R., Sharma, R. K., & Khan, M. S. (2024). Enhancement of cyber security in IoT based on ant colony optimized artificial neural adaptive Tensor flow. Network: Computation in Neural Systems, 1–17. https://doi.org/10.1080/0954898X.2024.2336058
14. Fraihat, S., Makhadmeh, S., Awad, M., Al-Betar, M. A., & Al-Redhaei, A. (2023). Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm. Internet of Things, 22, 100819. https://doi.org/10.1016/j.iot.2023.100819
15. Ghanem, W. A. H., Jantan, A., Ghaleb, S. A. A., & Nasser, A. B. (2020). An efficient intrusion detection model based on hybridization of artificial bee colony and dragonfly algorithms for training multilayer perceptrons. IEEE Access, 8, 130452–130475. https://doi.org/10.1109/ACCESS.2020.3009533
16. Pan, K. (2024). Research on network information security algorithms based intrusion detection using deep learning. In: 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), pp. 1–5. IEEE. https://doi.org/10.1109/ICICACS60521.2024.10499058
17. Kalyanaraman, K., & Prabakar, T. N. (2024). Enhancing women’s safety in smart transportation through human-inspired drone-powered machine vision security. In: AI Tools and Applications for Women’s Safety, pp. 150–166. IGI Global. https://doi.org/10.4018/979-8-3693-1435-7.ch009
18. Chiba, Z., Abghour, N., Moussaid, K., & Rida, M. (2019). Intelligent approach to build a deep neural network based IDS for cloud environment using combination of machine learning algorithms. Computers & Security, 86, 291–317. https://doi.org/10.1016/j.cose.2019.06.013
19. Alsarhan, A., Alauthman, M., Alshdaifat, E. A., Al-Ghuwairi, A. R., & Al-Dubai, A. (2023). Machine learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. Journal of Ambient Intelligence and Humanized Computing, 14(5), 6113–6122. https://doi.org/10.1007/s12652-021-02963-x
20. Ponmalar, A., & Dhanakoti, V. (2022). Hybrid Whale Tabu algorithm optimized convolutional neural network architecture for intrusion detection in big data. Concurrency and Computation: Practice and Experience, 34(19), e7038. https://doi.org/10.1002/cpe.7038
21. Joshi, C., Ranjan, R. K., & Bharti, V. (2023). ACNN-BOT: An ant colony inspired feature selection approach for ANN based botnet detection. Wireless Personal Communications, 132(3), 1999–2021. https://doi.org/10.1007/s11277-023-10695-8
22. Mayuranathan, M., Saravanan, S. K., Muthusenthil, B., & Samydurai, A. (2022). An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique. Advances in Engineering Software, 173, 103236. https://doi.org/10.1016/j.advengsoft.2022.103236
23. Chompookham, T., Phiphitphatphaisit, S., Okafor, E., & Surinta, O. (2024). Robust model selection for plant leaf image recognition based on evolutionary ant colony optimization with learning rate schedule. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3457753
24. Liu, C., Wang, L., Zhang, Z., Xiang, C., Gu, Z., Wang, Z., & Wang, S. (2024). Unsupervised intrusion detection based on asymmetric auto-encoder feature extraction. IEICE TRANSACTIONS on Information and Systems, 107(9), 1161–1173. https://doi.org/10.1587/transinf.2024EDP7001
25. Ripon, S., GolamSarowar, M., Qasim, F., & Cynthia, S. T. (2020). An efficient classification of tuberous sclerosis disease using nature inspired PSO and ACO based optimized neural network. Nature Inspired Computing for Data Science, 1–28. https://doi.org/10.1007/978-3-030-33820-6_1
26. Qian, Y. (2024). Application of ant colony optimization improved clustering algorithm in malicious software identification. International Journal of Advanced Computer Science & Applications, (IJACSA), 15(1), 1031-1039.
27. Mehta, A., & Charaya, S. (2022). Classification of images using machine learning by integrating edge detection algorithm and compression with ACO. Neuro Quantology, 20(18), 747.
28. Yang, T., Chen, J., Deng, H., & He, B. (2024). A lightweight intrusion detection algorithm for IoT based on data purification and a separable convolution improved CNN. Knowledge-Based Systems, 304, 112473. https://doi.org/10.1016/j.knosys.2024.112473
29. Chintapalli, S. S. N., Singh, S. P., Frnda, J., Divakarachari, P. B., Sarraju, V. L., & Falkowski-Gilski, P. (2024). OOA-modified Bi-LSTM network: An effective intrusion detection framework for IoT systems. Heliyon, 10(8). https://doi.org/10.1016/j.heliyon.2024.e29410
30. Prashanth, S. K., Iqbal, H., & Illuri, B. (2023). An enhanced grey wolf optimisation–deterministic convolutional neural network (GWO–DCNN) model-based IDS in MANET. Journal of Information & Knowledge Management, 22(04), 2350010. https://doi.org/10.1142/S0219649223500107
31. Narengbam, L., & Dey, S. (2024). Anomaly-based intrusion detection system using Harris Hawks optimisation with a sigmoid neuron network. International Journal of Information and Computer Security, 24(1–2), 5–27. https://doi.org/10.1504/IJICS.2024.140219
32. Krishna, A. Y., Kiran, K. R., Sai, N. R., Sharma, A., Praveen, S. P., & Pandey, J. (2023). Ant colony optimized XGBoost for early diabetes detection: A hybrid approach in machine learning. Journal of Intelligent Systems and Internet of Things, 10(02), 76–89. https://doi.org/10.54216/JISIoT.100207
33. Jayasankar, T., KirubaBuri, R., Maheswaravenkatesh, P. (2024). Intrusion detection system using metaheuristic fireworks optimization based feature selection with deep learning on Internet of Things environment, Journal of Forecasting, 43(2), 415–428. https://doi.org/10.1002/for.3037
34. Abdullah, D. (2024). Enhancing cybersecurity in electronic communication systems: New approaches and technologies. Progress in Electronics and Communication Engineering, 1(1), 38–43. https://doi.org/10.31838/ECE/01.01.07
35. Uvarajan, K. P. (2024). Advanced modulation schemes for enhancing data throughput in 5G RF communication

networks. SCCTS Journal of Embedded Systems Design and Applications, 1(1), 7–12. https://doi.org/10.31838/ESA/01.01.02

36. Siti, A., & Putri, B. (2025). Enhancing performance of IoT sensor network on machine learning algorithms. Journal of Wireless Sensor Networks and IoT, 2(1), 13–19.
37. Kavitha, M. (2024). Enhancing security and privacy in reconfigurable computing: Challenges and methods. SCCTS Transactions on Reconfigurable Computing, 1(1), 16–20. https://doi.org/10.31838/RCC/01.01.04
38. Kumar, T. M. S. (2024). Integrative approaches in bioinformatics: Enhancing data analysis and interpretation. Innovative Reviews in Engineering and Science, 1(1), 30–33. https://doi.org/10.31838/INES/01.01.07