Journal of Intelligent Systems and Internet of Things
Vol. 17, No. 02, PP. 101-118, 2025
DOI: https://doi.org/10.54216/JISIoT.170208

Ensemble Learning-Based Intrusion Detection and Classification for Securing IoT Networks: An Optimized Strategy for Threat Detection and Prevention

Kumaresh Sheelavant[1], Charan K. V.[2], B. Yamini Supriya[3], Purshottam J. Assudani[4], Chandra Bhushan Mahato[5], Sanjay Kumar Suman[6,*]

[1]Associate Professor, Dept. of CSE (AI&ML), Sai Vidya Institute of Technology, Visvesvaraya Technological University, Bengaluru, Karnataka, India

[2]Associate Professor, Dept. of ISE, Shridevi Institute of Engineering and Technology, Visvesvaraya Technological University, Karnataka, India

[3]Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

[4]Assistant Professor, School of Computer Science and Engineering, Ramdeobaba University, Nagpur, Maharashtra, India

[5]Principal, MIT Muzaffarpur, Bihar, India

[6]Professor, Dept. of AI&DS, Sri Shanmugha College of Engineering and Technology And Director Research, Sri Shanmugha Educational Institutions, Sankari, Salem, TN, India

Emails: kumaresh.s@saividya.ac.in; charan.kv@shrideviengineering.org; yamini.bommisetti@gmail.com; pjassudani@gmail.com; cbmahto1960@gmail.com; director.research@shanmugha.edu.in

Abstract

The Internet of Things (IoT) advancement has created new security holes, which require intrusion detection systems to defend networks effectively. The complex structure of IoT networks causes traditional security methods to fail because they produce high amounts of incorrect detections and limited ability to accurately identify threats. The authors introduce ID-ELC: Ensemble Learning and Classification framework for Intrusion Detection, which aims to strengthen IoT environment security. A new ID-ELC model uses CS optimization with composite variance to choose network features that boost their detection capabilities. The cybersecurity evaluation of the system utilized Kyoto network records that included 91,000 intrusion-prone records and 59,000 benign logs from 150,000 total records. Experiments revealed ID-ELC surpasses Statistical Flow Features (SFF) and Two-layer Dimension Reduction and Two-tier Classification (TDRTC) through precision 0.98, accuracy 0.98, sensitivity 0.99 and specificity 0.97. Science-based evaluations confirm ID-ELC represents a flexible and resilient tool for IoT intrusion protection that shows practical value for citywide security systems and medicine networks and manufacturing operations. Future investigation will concentrate on enhancing the selection of features alongside classification methods to address rising cyber threats.

Received: January 19, 2025 Revised: March 17, 2025 Accepted: May 30, 2025

Keywords: Intrusion Detection System (IDS); Machine Learning; Internet of Things (IoT); Cybersecurity; Cuckoo Search Algorithm (CS); Statistical Flow Features (SFF); TDRTC; Kyoto Dataset; Feature Optimization

1. Introduction

Modern technology experienced a breakthrough through the Internet of Things (IoT) which connects billions of devices, which talk effortlessly between devices as well as with human users. Different types of devices featuring sensors and smart technologies now exist across industries as well as healthcare facilities and homes and transportation systems and critical infrastructure networks [1]. Research indicates the number of IoT devices with

internet connections reached more than 30 billion by 2020 as funding reached $6 trillion. A remarkable increase in IoT adoption brought convenient operations alongside severe security dangers to the market.

The combination of advanced functionalities and slim computational capabilities within IoT devices makes them exposed to cyber threats. Attacks happen through security vulnerabilities that enable unauthorized control or database modifications as well as substantial network disruption [2]. The combination of security vulnerabilities in IoT devices creates major dangers that become especially dangerous when such devices operate in essential domains like smart cities and industrial automation and healthcare systems. Security measures for IoT networks have risen to the top research priorities for global authorities including governmental bodies and organizations.

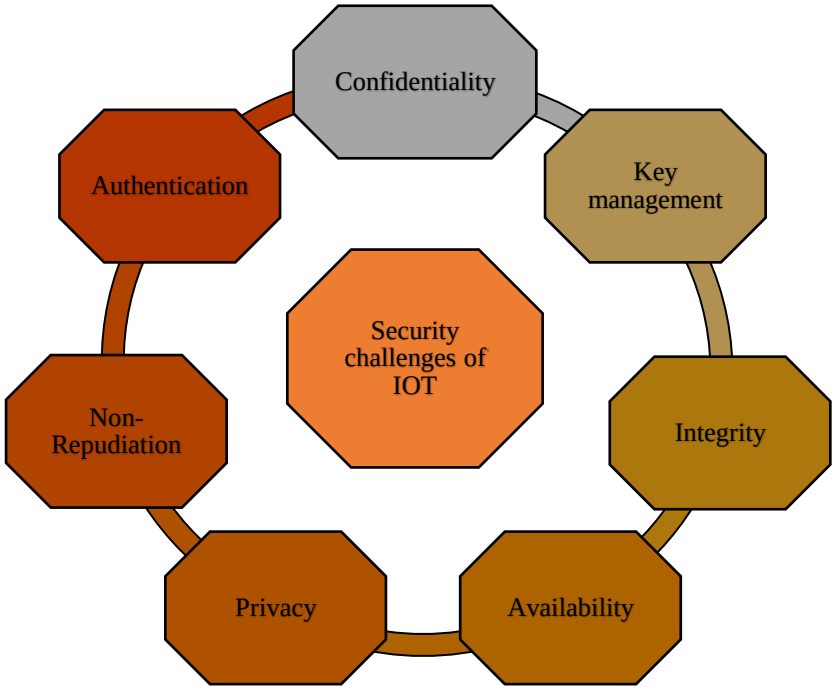

Figure 1. IoT Network Security Challenges

Figure 1 shows the key security challenges that IoT technologies encounter including confidentiality, integrity, privacy, availability, authenticity, non-repudiation, and key management.

1.1 Intrusion Threats in IoT Networks

The intrusions affecting IoT networks take many shapes including malware infections together with Distributed Denial of Service (DDoS) attacks and advanced botnets as well as unauthorized data theft. Security vulnerabilities unique to IoT networks exist because these systems contain different hardware structures together with minimal processing capacity and non-standard security measures [3]. Attackers take advantage of these vulnerabilities to carry out cyber threats by focusing on IoT sensors as well as gateways and cloud-based applications.

IoT security faces two major threats, which include:

- Malware-Based Attacks – Ransomware together with worms spreads within IoT networks to take control of devices so attackers can perform harmful actions [4]. Botnets, which consist of compromised IoT devices, can execute big-scale DDoS attacks.
- Man-in-the-Middle Attacks (MITM) – Attackers steal IoT device server traffic for surveillance purposes and they both examine and change send data by adding harmful information to the network flow [5].
- Unauthorized Access and Data Breaches – The lack of adequate authentication in IoT devices creates security holes through which attackers can enter and steal sensitive data as well as acquire control of connected systems.

- Sensor-Based Attacks – Attackers who exploit sensors in IoT setups can use these weaknesses to change data values, which leads to bogus security warnings and system operational interruptions in vital programs such as hospital medical surveillance or factory automation systems.
- Protocol-Level Exploits – The security of numerous IoT devices is compromised because various devices continue operating with low-grade security protocols that lack both encryption and authentication features.

Security risks for IoT applications become greater because of their numerous use cases and their connection to public networks [5]. Open operating conditions of IoT devices prevent users from implementing robust security protocols due to networking challenges.

1.2 Need for Advanced Intrusion Detection in IoT Networks

The combination of firewalls and antivirus software along with routine encryption methods proves inadequate for safeguarding Internet of Things networks. Security mechanisms must be both proactive and adaptive since IoT devices form an enormous network and their usage patterns change frequently. Intrusion Detection Systems (IDS) serve as the solution for protecting IoT networks [6]. The IDS system maintains active monitoring of network traffic and identifies irregular activities alongside spotting potential security threats, which help, prevent major damages.

Multiple detection strategies exist for IoT network intrusion prevention.

- Signature-Based Detection: The system evaluates incoming traffic patterns through established attack signature databases [7]. IDS detection methods continue to protect known threats yet they show weakness against developing or unknown attack patterns.
- Anomaly-Based Detection: The system uses statistical models together with machine learning techniques to monitor abnormal system activities [8]. Companies use this technique to discover cyber-attacks that were not previously detected.
- Hybrid Detection Models: The system integrates various detection methods so users achieve higher detection precision as well as lower incorrect alarming rates.

Designing a lightweight yet effective ID represents the main security challenge specific to IoT devices [9]. The ideal IDS for IoT devices need to have accurate detection capabilities that do not cause significant computational burden because many IoT devices operate with restricted processing power.

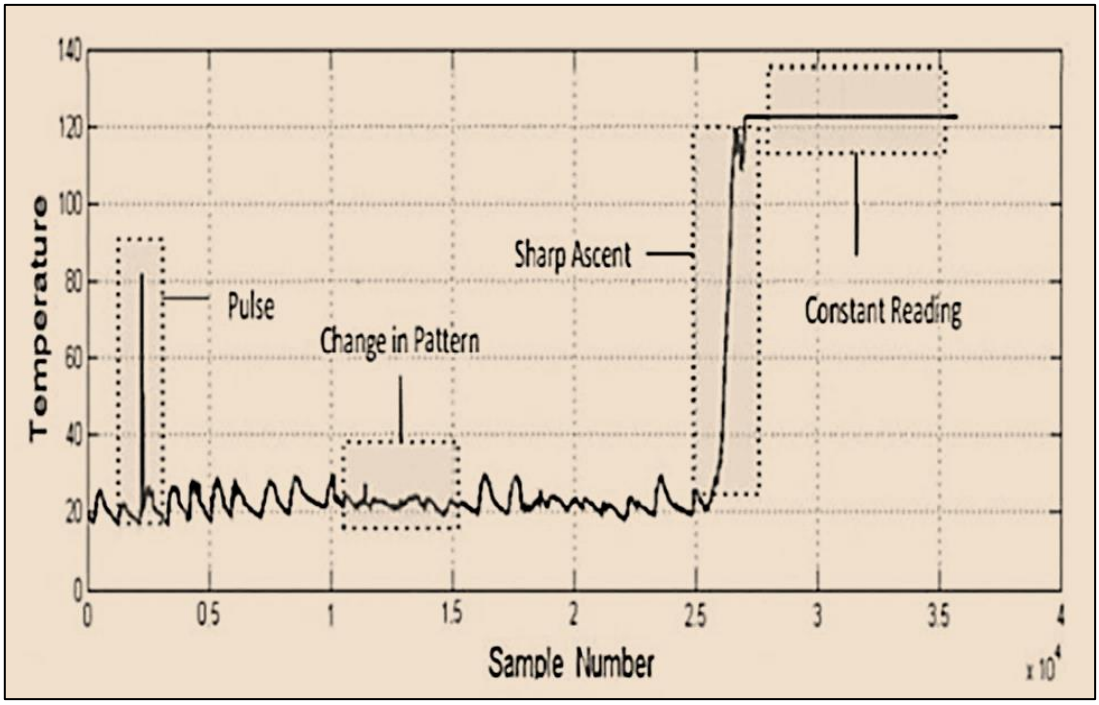

Figure 2. Appearance of anomalies in the information

The Figure 2 demonstrates different anomalies found in IoT data systems that are essential for detecting security breaches.

1.3 Machine Learning and Ensemble Learning in IoT Security

Intrusion detection within IoT networks utilizes machine learning to become an effective operational tool. Through machine learning algorithms a large quantity of network data becomes detectable as patterns matching cyberattack behaviour and potential security threats [10]. The supervised and unsupervised learning methods in IDS allow the system to distinguish between normal and suspicious traffic, which improves its detection capacity.

Ensemble learning proves to be a key development in IoT security by using several machine-learning models, which enhance classification results. The combination of individual models through ensemble methods produces extremely reliable intrusion detection systems that utilize strengths and resolve weaknesses between components [11]. Popular ensemble techniques include:

- Bagging (Bootstrap Aggregating): The system uses multiple models processing diverse portions of the data, which are merged into one prediction to lower prediction variations and enhance prediction accuracy.
- Boosting: The system uses previous model error correction methods to advance detection accuracy across the board.
- Stacking: This method uses a separate decision-making model to analyse the output of various classifiers to generate new predictions.

Multiple cybersecurity applications achieve top performance levels through ensemble learning because this method surpasses individual model detection methods [12]. The implementation of IoT intrusion detection systems benefits from ensemble learning because it delivers better detection capability with lower false positive rates alongside the ability to handle new security threats.

The fast-growing IoT infrastructure now requires research focus on intrusion detection techniques because of its complex security challenges [13]. The current IoT environments require beyond traditional security methods because these methods cannot handle their dynamic and large-scale characteristics. Computer learning and ensemble computing methods provide effective solutions to identify and control cyber threats [14]. The implementation of advanced IDS frameworks enables organizations to achieve better IoT security which results in dependable operations of connected devices.

2. Related Work

The expanding Internet of Things operational space requires IDS systems to protect IoT devices because their rapid growth produces security risks. Different detection and mitigation methods have been developed for cyberattacks through mechanisms that preserve both low resource usage and high accuracy rates. The detection methods extend from statistical evaluation to machine learning when combined with hybrid models [15]. The survey evaluates multiple intrusion detection methodologies as well as their strengths and weaknesses for IoT systems.

2.1 Intrusion Detection Techniques

The detection of intrusions occurs through three main categories including statistical-based methods combined with clustering techniques together with machine learning-based approaches. The detection of malicious activities in IoT networks benefits from the different attributes and borders that each detection method provides [16].

- Statistical-Based Techniques: Information on network activities serves as input for statistical methods that reveal abnormal events that may point to a security breach. The set of statistical models for intrusion detection features Hidden Markov Models (HMM), Naïve Bayes classifiers in addition to distance measurement techniques and multivariate correlation analysis [17]. The detection methods use predefined threshold definitions for anomaly identification. The detection effectiveness of these methods remains high yet they produce numerous incorrect alarms because of network behaviour variation.
- Clustering-Based Techniques: Network traffic organizations through clustering enable security systems to distinguish between standard and threatening activities. Many organizations utilize three clustering techniques including K-means clustering and Optimum-path Forest classification alongside subspace clustering for their intrusion detection efforts [18]. Zero-day attacks get identified effectively through these methods because they avoid using preset attack signatures. These detection methods experience measurement imprecision because of continuous behavioural changes that occur in IoT network environments.

2.2 Machine Learning-Based Approaches

Machine learning techniques serve intrusion detection purposes using supervised and unsupervised learning models extensively.

- Supervised Learning Techniques: Supervised learning devices use labeled datasets for training since this method effectively detects recognized attack signatures. The main types of intrusion detection classifiers are Support Vector Machines (SVM) alongside Decision Trees and Random Forests. The classification methods achieve excellent rates in discovering Denial of Service (DoS) attacks alongside probing attack types [19]. Their ability to detect new attack types is constrained because they need predefined labels for operation.
- Unsupervised Learning Techniques: The detection of network traffic by self-organizing maps and autoencoders takes place without needing predefined labels [20]. Among the clustering methods K-Means and hierarchical clustering form this category of algorithms. The detection of new attacks is possible with these models yet they produce more false alarms than supervised approaches do.
- Hybrid Machine Learning Approaches: Detection rates gain improvement through the combination of supervised and unsupervised learning applied in hybrid techniques. IDS systems with two stages accomplish known attack detection through rules before employing machine learning to decrease incorrect positive and negative results [21]. Attacks need deep learning analysis by implementing Convolutional Neural Networks (CNNs) along with Recurrent Neural Networks (RNNs).

2.3 Feature Selection and Reduction Methods

The selection process for features stands as a vital component for improving the operational effectiveness of intrusion detection models [22]. PCA and Fisher Dimension Reduction methods serve to eliminate superfluous features thus achieving better efficiency with no impact on detection success rates. Mutual information-based approaches have been utilized to find the most crucial attributes for achieving classification purposes. The performance-improving techniques show limitations when detecting different attack patterns due to their reduced accuracy level [23].

2.4 Intrusion Detection in Cloud-Based and Industrial IoT Environments

IoT security threats now encompass both cloud platforms as well as manufacturing environment systems. Cloud computing systems require their intrusion detection systems to efficiently handle large-scale data streams together with effective prevention of false alarms [24]. Cloud service DDoS prevention uses multivariate correlation evaluation together with ensemble-based methods for feature choice.

Becoming essential for industrial operations involves protecting both Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) network systems. Hybrid IDS uses Hidden Markov Models as well as additional approaches to differentiate between operational anomalies and cyber intrusions [25]. The security solutions enhance robustness in essential infrastructures although they need regular adjustments to counter the latest threats.

2.5 IoT-Specific Security Challenges and Emerging Solutions

IoT networks create distinctive security problems, which result from their dynamic nature and their resource-limited architecture with heterogeneous platforms and changing attack strategies. Current network intrusion detection methods that use predefined code profiles struggle to detect fresh attack techniques that are unidentified yet known as zero-day attacks [26]. The large amount of data from IoT operations makes it more difficult to handle detection procedures.

Researchers aim to solve these security issues through developmental security frameworks based on artificial intelligence. Specific intrusion detection and prevention software models based on machine learning technology predict threats while automatically detecting them before taking necessary self-driven action without human interaction [27]. Distributed IoT networks benefit from two innovative security solutions represented by blockchain authentication methods and federated learning techniques [28-29].

The detection of intrusions in IoT networks needs statistical analysis and machine learning techniques to operate with adaptive security measures [30-31]. Technology developers have built different detection systems yet they must resolve ongoing trade-offs between system accuracy of detection and speed of operation and response to novel security threats. Future examinations need to establish novel IDS models and intelligent detection mechanisms that detect and counter cyberattacks during IoT network developments [32].

3. Objectives of Research

The research creates an Ensemble Learning and Classification (ID-ELC) system to improve IoT network intrusion detection capabilities. The quick expansion of IoT networks has led to more security threats especially in the form of botnet attacks thus requiring advanced detection systems.

The research has four main objectives.

- The goal of this research is to develop an Intrusion Detection system, which enhances malicious traffic detection abilities in IoT networks.
- The combination of composite variance along with cuckoo search algorithms provides a method to optimize the selection process for network data analysis.
- A combination of ensemble learning approaches helps both cut down false-positive detection mistakes and enhance the accuracy of interferences recognition.
- The model undergoes testing on actual world datasets that proves its better performance compared to current detection approaches.

Research findings demonstrate that ID-ELC provides a strong and expandable detection system that achieves superior results over conventional security methods. Additional study on sophisticated classification processes should proceed to advance cybersecurity protection according to this research.

4. Motivation of the Research

The wide spread of Internet of Things devices now requires organizations to focus on effective intrusion detection because security threats have grown rapidly. The vulnerability of IoT devices makes them susceptible to botnet attacks, which exploit network flaws to launch big-scale interference. Intrusion detection mechanisms based on traditional systems fail to identify legitimate from malicious network traffic because of complex IoT network structures.

The investigation drives from a need to create improved threat identification systems that deliver prompt alerts along with optimum accuracy. The proposed research uses ensemble capabilities together with optimized selection features to improve detection precision in intrusions.

Protecting IoT networks has become essential because these networks are used extensively in three major sectors including healthcare, smart cities, and industry. The research intends to develop an adaptable intrusion detection system framework that operates on a large scale to cope with emerging cyber threats for enhancing IoT security.

5. Proposed Work

Technology has undergone substantial transformation because of the Internet of Things (IoT) leading to massive systems apartness. Distributed operation of IoT systems produces a multitude of security risks. A considerable number of IoT devices function insecurely because of their basic security setup that leaves them exposed to Distributed Denial of Service (DDoS) attacks as well as malware infections and botnet-based intrusions. IDS systems have limited capacity to identify and respond to the characteristics of heterogeneous IoT networks operating with high traffic volume.

The proposed research develops an Intrusion Detection using Ensemble Learning and Classification (ID-ELC) to detect benign and malicious traffic patterns by applying ensemble classification methods with statistical flow features while optimizing feature selection.

The proposed system consists of:

- The proposed system adopts Feature Selection and Optimization to establish the most critical attributes.
- Ensemble Learning: Combining multiple classifiers for improved accuracy.
- Classification efficiency works through the Hierarchical Nesting Mechanism, which implements feature structure for organization.
- Light classification assigns labels by using voting procedures based on probabilities for decision-making purposes.

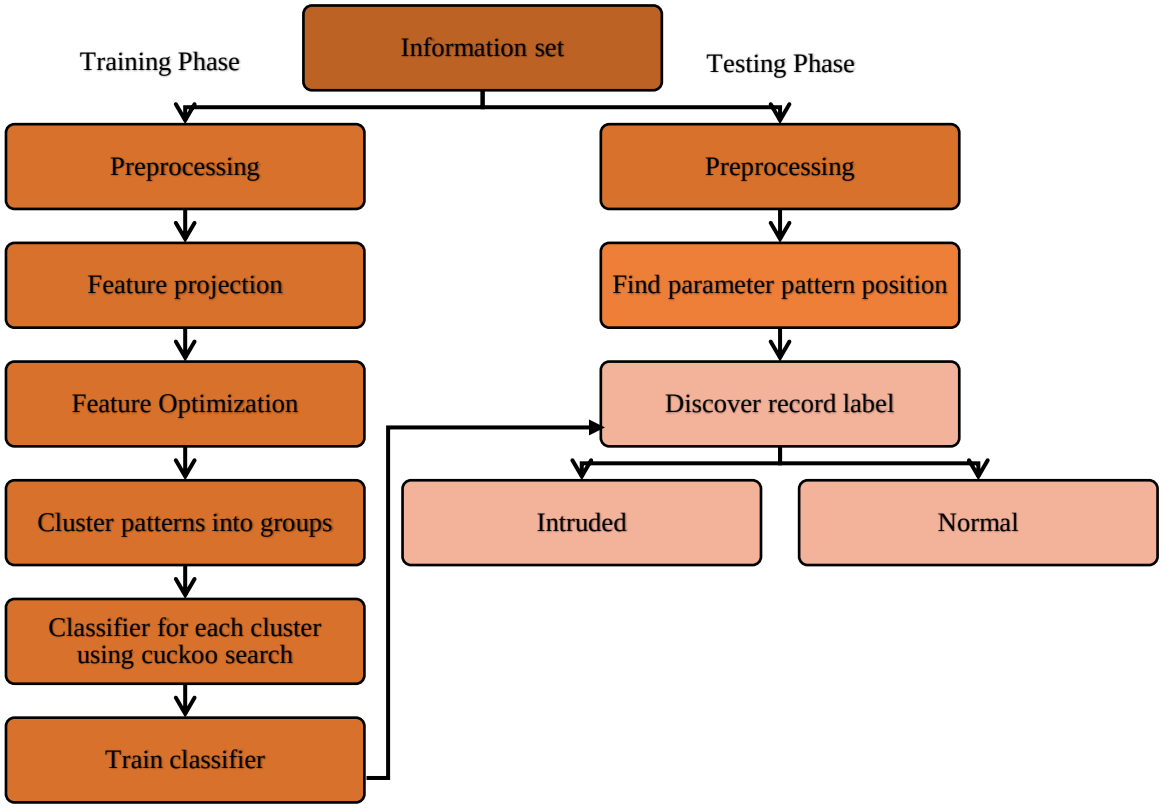

Figure 3. Block illustration of proposed ID-ELC approach

5.1 Feature Selection and Optimization

The process of feature selection stands essential for intrusion detection systems at IoT environments due to their generation of vast network traffic data with numerous attributes. The process of picking representative features and discarding redundancies and noisy data components leads to better accuracy levels in classifications along with decreased computational demands and faster threat detection during real-time operations. The proposed Intrusion Detection by Ensemble Learning and Classification (ID-ELC) framework employs Composite Variance Analysis and the Cuckoo Search Algorithm (CS) for feature optimization. The techniques select the most important features to use for intrusion detection, which leads to improved performance in machine learning models.

5.1.1 Composite Variance Analysis for Feature Ranking

A statistical method called Composite Variance determines the distance between benign and malicious traffic patterns to find key features for classification. Analysis of variance evaluates numerical features in both benign and malicious traffic groups independently in a dataset.

The feature vectors, which represent benign and malicious traffic patterns, are notated as v1 and v2. The composite variance expresses as formula:

$$CV(v_1, v_2) = \frac{|\mu(v_1) - \mu(v_2)|}{\sigma(v_1) + \sigma(v_2)} \quad (1)$$

Here μ(v) = mean of feature, σ(v) = standard deviation.

$$\mu(v) = \frac{1}{N}\sum_{i=1}^{N} v_i \quad (2)$$

$$\sigma(v) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(v_i - \mu(v)\right)^2} \quad (3)$$

The strength of a feature for selection depends on the value of its composite variance because higher figures show substantial benign versus malicious traffic distinctions. Features characterized by low variance play a minimal role in classification so they become candidates for elimination.

5.1.2 Cuckoo Search Algorithm for Feature Optimization

Cuckoo Search uses ranking features as its input to execute optimization. The brood parasitism behaviour of cuckoo birds serves as the foundation for Cuckoo Search (CS), which represents a natural optimization method. The algorithm improves feature subsets through an iterative process to select important features and remove unnecessary attributes.

The Lévy flight distribution pattern directs the random exploration of feature subsets that takes place during CS searches. The new solution for feature subset improvement follows this rule:

$$x_i^{(t+1)} = x_i^{(t)} + \alpha \times Levy(\lambda) \quad (4)$$

Here $x_i^{(t)}$ = current feature subset, α = step size.

Lévy flight follows a probability distribution given by:

$$Levy(\lambda) \sim u = t^{-\lambda}, 1 < \lambda \leq 3 \quad (5)$$

The evaluation of feature subsets occurs through fitness function assessments that aim to achieve maximum classification accuracy at each loop.

$$FF = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

The system classifies results based on TP, TN, FP and FN statistics. The system maintains the most effective feature subsets from selection while tossing out underperforming ones to find the best classification feature set.

5.2 Ensemble Learning for Classification

Machine learning performance suffers because of low accuracy rates when one classifier attempts to detect mixed IoT network traffic patterns. The detection process employing ensemble learning uses several classifiers for improving overall performance alongside lowering weaknesses through multiple classifier usage. ID-ELC implements a set of several classifiers, which incorporate Decision Trees (DT), Support Vector Machines (SVM), Random Forests (RF) and K-Nearest Neighbors (KNN).

5.2.1 Construction of the Ensemble Model

The ensemble contains classifiers that receive training from different selected subset features chosen through optimization processes. A voting process analyzes multiple classification outputs through weighted systems to identify the final forecast result. The ensemble model produces y by computing a prediction through each classifier hi(x) on the input traffic sample x.

$$y = \arg max \sum_{i=1}^{n} w_i h_i(x) \quad (7)$$

Here w_i = weight assigned to each classifier, $h_i(x)$ = classification outcome.

5.2.2 Classifier Weighting and Decision Fusion

The runtime adjustment of weights for each classifier occurs because of real-time metrics evaluations. The weight update formula is:

$$w_i = \frac{Accuracy\ of\ h_i}{\sum_{j=1}^{n} Accuracy\ of\ h_j} \quad (8)$$

The model implementation technique gives accuracy-based weights to classifiers that enhance their weight in producing final prediction results.

5.2.3 Decision Trees (DT)

The hierarchical model known as Decision Tree fulfills classification demands by splitting data recursively through feature values. The method contains decision points expressed as nodes and final class identification indicated by leaves. The Gini impurity serves as a purity measurement for tree divides while the best attribute selection drives tree expansion. The if-else rule system drives decision-making within Decision Trees leading to interpretability yet leading to excessive model fitting.

$$Gini = 1 - \sum p_i^2 \quad (9)$$

$$E = -\sum p_i \log_2 p_i \quad (10)$$

5.2.4 Support Vector Machines (SVM)

The classifier known as Support Vector Machines (SVMs) enables high-dimensional data point partitioning through hyperplane separation. Support vectors function as critical data points to create optimal class separation margins that function as the classification goals for SVMs. SVM creates a determination boundary from input data x that follows:

$$f(x) = w \cdot x + b \quad (11)$$

The solution of the optimization problem happens with the help of Lagrange multipliers. SVM uses kernel functions such as Radial Basis Function (RBF) to successfully process data sets that cannot be separated by linear boundaries.

5.2.5 Random Forests (RF)

Random Forest constitutes an ensemble-learning framework that achieves high accuracy through the combination of numerous Decision Trees. Each of the trees receives its own random subset of data obtained through Bootstrap Aggregation (Bagging). The majority voting approach determines the final prediction.

$$y = \text{mode}\big(h_1(x), h_2(x), \ldots, h_n(x)\big) \quad (12)$$

RF decreases prediction errors and delivers better performance than individual Decisions Trees.

5.2.6 K-Nearest Neighbors (KNN)

The non-parametric classification technique K-Nearest Neighbors (KNN) identifies data point labels through the majority voting of k closest neighbors to it. The method for determining point distance in KNN employs Euclidean distance:

$$d(x, y) = \sqrt{\sum (x_i - y_i)^2} \quad (13)$$

Despite its effectiveness, KNN performs slowly on large dataset processing. Performance outcomes heavily depend on selecting the best value of k.

Here p_i = probability of class, w = weight, b = bias, $h_i(x)$ = individual tree prediction,

5.3 Classification and Decision Making

The classification process labels incoming network traffic samples through the trained ensemble model and determination of benign or malicious classes. The final decision follows a process of probability calculations from individual classifiers and output combination to produce the final choice.

5.3.1 Probability Computation for Classification

The determination of a sample R as malicious is based on the following probability:

$$P_{attack}(R) = \frac{\sum_{i=1}^{n} P_i(R) \cdot w_i}{\sum_{i=1}^{n} w_i} \quad (14)$$

The probability for benign samples can also be determined through the same formula.

$$P_{benign}(R) = 1 - P_{attack}(R) \quad (15)$$

5.3.2 Final Decision Rule for Label Assignment

A sample is classified as malicious if:

$$P_{attack}(R) > P_{benign}(R) \quad (16)$$

The sample requires additional examination when $P_{attack}(R)$ is approximately equal to $P_{benign}(R)$.

5.3.3 Handling Uncertainty and False Positives

Investigators introduced the confidence threshold τ to decrease erroneous positive results in this method.

$$if \left| P_{attack}(R) - P_{benign}(R) \right| < \tau \quad (17)$$

The validation process establishes additional testing requirements for samples with uncertain results to achieve proper classification.

5.4 ID-ELC Algorithm

ID-ELC Intrusion Detection algorithm

Input: IoT Network Traffic Dataset D

Output: Classified Traffic (Benign/Malicious)

The dataset D requires normalization and noise elimination as part of its preprocessing stage.
The system extracts statistical information based on flow data from network packets.
The system applies Composite Variance Analysis for feature ranking.
The adoption of Cuckoo Search Algorithm optimizes the feature selection process.
Initialize feature nests randomly.
Evaluate fitness using classification accuracy.
The model employs Lévy flight mechanism to discover brand new features during the generation process.
A process to replace weak-performing nests with cutting-edge solutions should be implemented.
Repeat until convergence.
The optimized features will be used to train ensemble classifiers including DT, SVM, RF, KNN.
Compute classifier weights dynamically.
Apply the ensemble model to test newly obtained traffic samples.
Finally determine the classification probabilities to establish the final class label.
Output classified network traffic.

Through the ID-ELC framework enabled intrusion detection systems obtain better results for IoT networks by utilizing ensemble learning with optimized feature selection. The detection system becomes more thanks that are accurate to improved security surveillance and minimal incorrect alerts through this framework. Research programs will study automatic learning approaches to deal with altering security threats.

6 Results

A comprehensive evaluation of the Intrusion Detection by Ensemble Learning and Classification (ID-ELC) framework needs performance analysis to assess its effectiveness. The system performs tests using a major-scale dataset from IoT networks to determine its accuracy measurements along with precision and sensitivity and specificity levels and general classifying effectiveness. ID-ELC undergoes performance assessment using a set of machine learning evaluation metrics against other existing intrusion detection systems. The experimental conditions use cross-validation with statistical evaluation methods for performing objective benchmarking. The research findings demonstrate how the model works in practice and its capabilities regarding scalability and real-world threat defence of IoT systems.

6.1 Accuracy

The percentage relation between correctly identified instances from both benign and malicious categories forms accuracy's measurement among all instances. The overall performance of a classifier gets its fundamental evaluation through this important measurement.

$$Accuracy = \frac{CP+CN}{TP} \quad (18)$$

6.2 Precision

The precision indicator determines the proportion of correctly detected malicious instances from all predictions. The metric remains critical for systems with high alarm costs because it decreases the number of incorrect alerts appearing to security personnel.

$$Precision = \frac{CP}{CP+IP} \quad (19)$$

6.3 Sensitivity

The recall sensitivity determines a model's ability to properly detect genuine malicious incidents. The metric determines how many of the correctly identified attacks exist within the total number of actual attacks.

$$\text{Sensitivity} = \frac{CP}{CP+IN} \quad (20)$$

6.4 Specificity

The model shows its quality in correctly identifying real benign instances through specificity. The algorithm establishes the percentage ratio between correct benign traffic identifications.

$$\text{Specificity} = \frac{CN}{CN+IP} \quad (21)$$

6.5 F1-Score

The F1-score calculates the precision and recall values by using their harmonic mean. The F1-Score serves to balance errors between false alarm detection and mistaken negatives by offering a solution for datasets that present with current imbalances.

$$F1 - Score = 2 * \frac{Precision * Specificity}{Precision + Specificity} \quad (22)$$

6.6 Matthews Correlation Coefficient (MCC)

MCC presents a fair method of classifying performance that works best on imbalanced datasets and their classification needs. The assessment method looks at all four elements of the confusion matrix while rating matrices between -1 and 1.

$$MCC = \frac{(CP \times CN) - (IP \times IN)}{(CP+IP)(CP+IN)(CN+IP)(CN+IN)} \quad (23)$$

Here CP = correct positive, CN = correct negative, IP = incorrect positive, IN = incorrect negative.

Table 1: Evaluation of compared Accuracy of existing approach with suggested approach

Fold ID	SFF	TDRTC	DNN-IDS	CNN-LSTM	Random Forest	SVM-Based IDS	ID-ELC (Proposed)
Fold 1	98.22	95.55	94.41	93.67	92.02	90.94	99.26
Fold 2	97.48	96.43	94.85	93.89	92.23	91.31	98.91
Fold 3	98.77	96.56	95.08	94.01	92.52	91.54	99.49
Fold 4	98.23	96.18	94.73	93.47	91.89	90.73	99.08
Fold 5	97.7	95.58	94.02	93.04	91.67	90.35	99.57

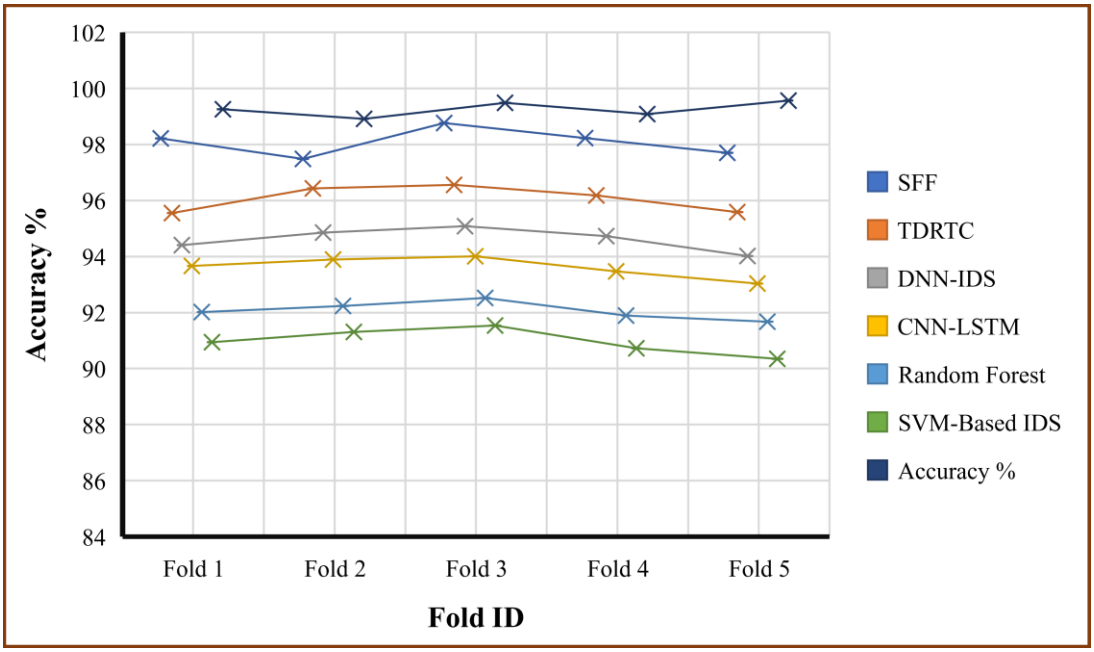

Figure 4. Graphical illustration of compared Accuracy

The accuracy data in the table 1 and Figure 4 shows that ID-ELC (Proposed) surpasses six established intrusion detection approaches with its performance across five different folds ranging between 98.91% and 99.57%. The ID-ELC model outperforms all other methods since it achieves 98.91% to 99.57% accuracy in each fold run. The accuracy level of SFF and TDRTC methods shows high performance at 97.48% and 98.77% while DNN-IDS,

CNN-LSTM, Random Forest and SVM-Based IDS demonstrate slightly lower results. Superior accuracy of the ID-ELC model shows its strong ability to detect malicious network traffic that results in enhanced reliability and robustness for intrusion detection in IoT environments.

Table 2: Evaluation of compared Precision of existing approach with suggested approach

Fold ID	SFF	TDRTC	DNN-IDS	CNN-LSTM	Random Forest	SVM-Based IDS	ID-ELC (Proposed)
Fold 1	98.21	95.53	93.98	93.11	91.74	90.25	99.26
Fold 2	97.45	96.41	94.47	93.56	92.03	91.09	99.25
Fold 3	98.76	96.59	94.99	93.74	92.42	91.48	99.33
Fold 4	98.22	96.17	94.58	93.13	91.85	90.79	99.44
Fold 5	97.71	95.56	93.85	92.87	91.61	90.32	99.87

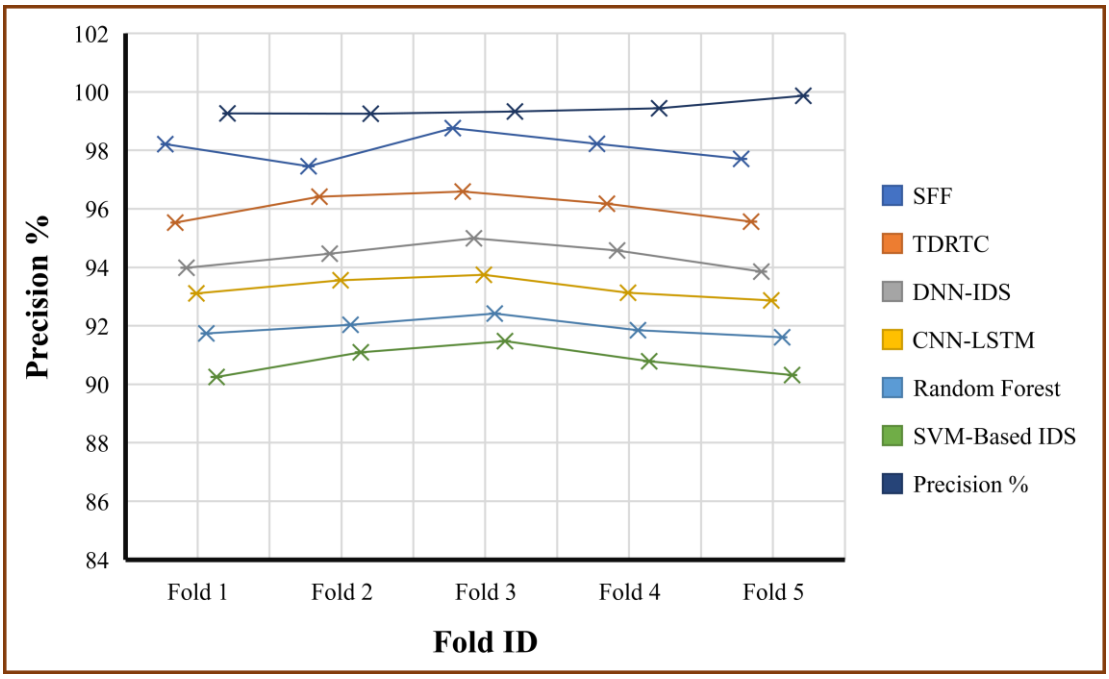

Figure 5. Graphical illustration of compared Precision

The precision results of ID-ELC (Proposed) against six existing intrusion detection approaches are shown in the table 2 and Figure 5 across five folds. The precision level of ID-ELC stays at the peak between 99.25% and 99.87% resulting in better performance than all competing models. All precision values from SFF and TDRTC surpass those of DNN-IDS, CNN-LSTM, Random Forest and SVM-Based IDS by remaining above 97.45% up to 98.76%. The superior precision performance of the ID-ELC model allows it to detect malicious traffic effectively with low false positive rates thus making it an optimal choice for IoT network security systems.

Table 3: Evaluation of compared Sensitivity of existing approach with suggested approach

Fold ID	SFF	TDRTC	DNN-IDS	CNN-LSTM	Random Forest	SVM-Based IDS	ID-ELC (Proposed)
Fold 1	96.4	92.1	90.42	89.47	88.45	87.23	99.9
Fold 2	95.3	93.1	90.85	90.04	88.62	88.08	99.3

Fold 3	97.8	94.4	91.56	90.59	89.01	88.5	99.9
Fold 4	96.7	93.3	91.24	90.12	88.79	87.89	99.4
Fold 5	97.9	92.7	90.03	89.07	88.01	87.05	98.76

Table 4: Evaluation of compared Specificity of existing approach with suggested approach

Fold ID	**SFF**	**TDRTC**	**DNN-IDS**	**CNN-LSTM**	**Random Forest**	**SVM-Based IDS**	**ID-ELC (Proposed)**
Fold 1	96.8	92.9	91.54	90.53	89.41	88.29	98.3
Fold 2	95.7	94.2	92.02	91.08	89.97	88.72	98.3
Fold 3	97.6	94.3	92.25	91.34	90.13	89.09	98.4
Fold 4	96.8	93.8	91.87	90.81	89.72	88.53	98.6
Fold 5	95.9	92.9	90.72	89.79	88.63	87.54	99.8

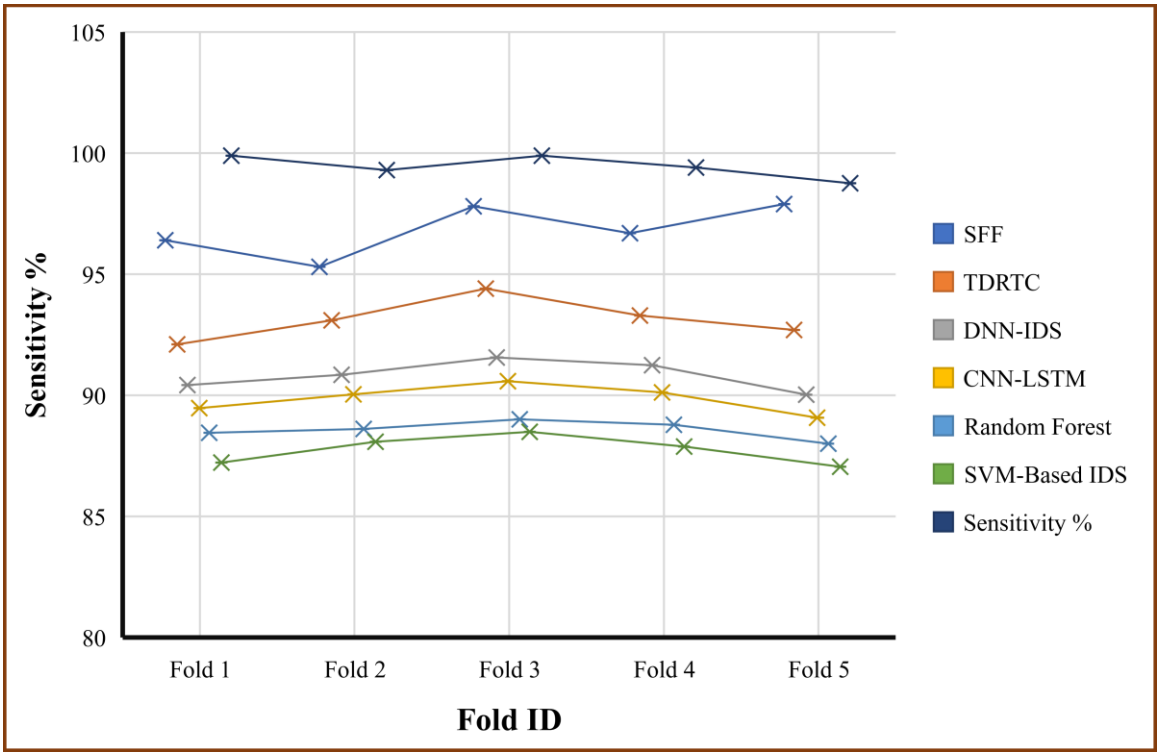

Figure 6. Graphical illustration of compared Sensitivity

The table 3 and Figure 6 evaluates the recall performance of the ID-ELC (Proposed) model against six intrusion detection approaches in five evaluation folds. The recall results from ID-ELC evaluation demonstrate the highest levels reaching between 98.76% and 99.9%, which establishes it as the most successful model. The recall scores of SFF and TDRTC fall between 95.3% and 97.9% but ID-ELC (Proposed) maintains a strong detection capability reaching 98.76% to 99.9% and outperforms all competing technologies in this evaluation. ID-ELC proves to be an effective solution for IoT security systems because its highest detection rate demonstrates its excellence in identifying malicious traffic.

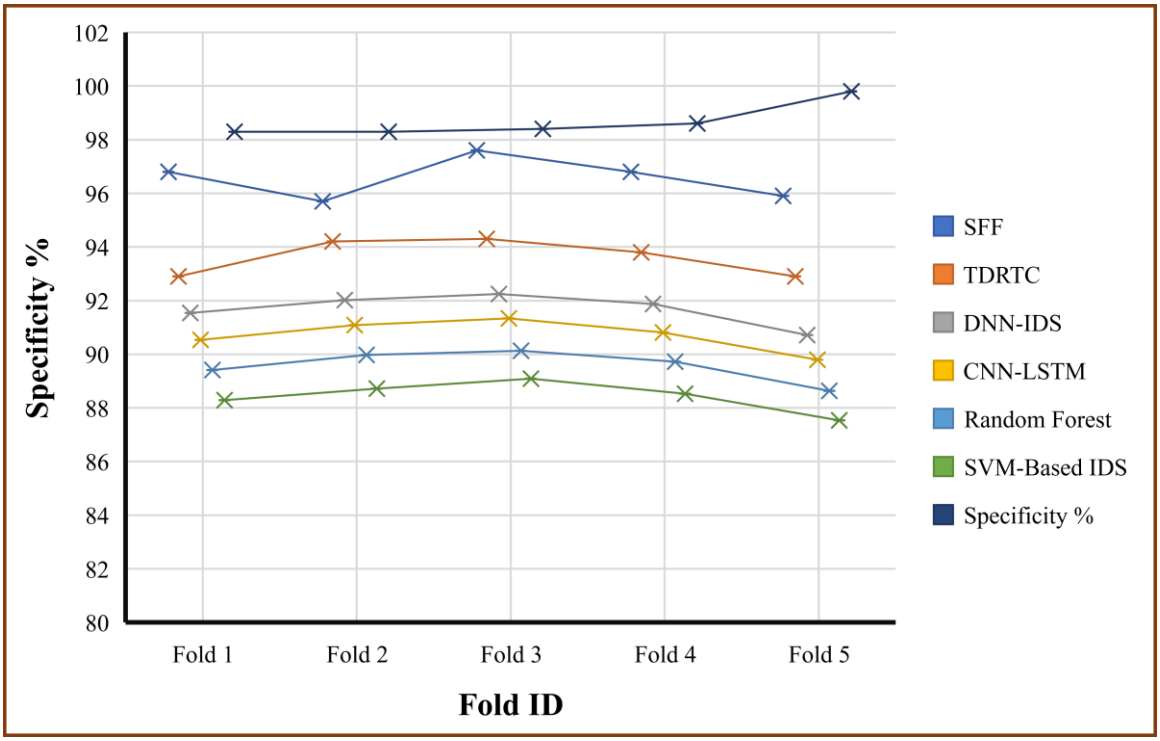

Figure 7. Graphical illustration of compared Specificity

The ID-ELC (Proposed) model shows better specificity than six established intrusion detection methods while monitoring five different rounds of data as shown in table 4 and Figure 7. ID-ELC exhibits the highest specificity between 98.3% and 99.8% that proves its exceptional ability to detect harmless traffic patterns with minimal wrong alarms. The specificity results for SFF and TDRTC lie between 95.7% and 97.6% whereas DNN-IDS, CNN-LSTM alongside Random Forest and SVM-Based IDS demonstrate lower specificity values. The high specificity of ID-ELC leads to fewer false alarms so it becomes an efficient and dependable system to secure IoT networks

.

Table 5: Evaluation of compared F1-Score of existing approach with suggested approach

Fold ID	**SFF**	**TDRTC**	**DNN-IDS**	**CNN-LSTM**	**Random Forest**	**SVM-Based IDS**	**ID-ELC (Proposed)**
Fold 1	97.5	94.21	92.74	91.56	90.31	89.14	98.78
Fold 2	96.58	95.3	93.37	92.52	90.72	89.97	98.77
Fold 3	98.18	95.42	93.75	92.86	91.03	90.21	98.86
Fold 4	97.51	94.97	93.49	92.35	90.45	89.53	99.02
Fold 5	96.79	94.22	92.68	91.67	89.83	88.95	99.83

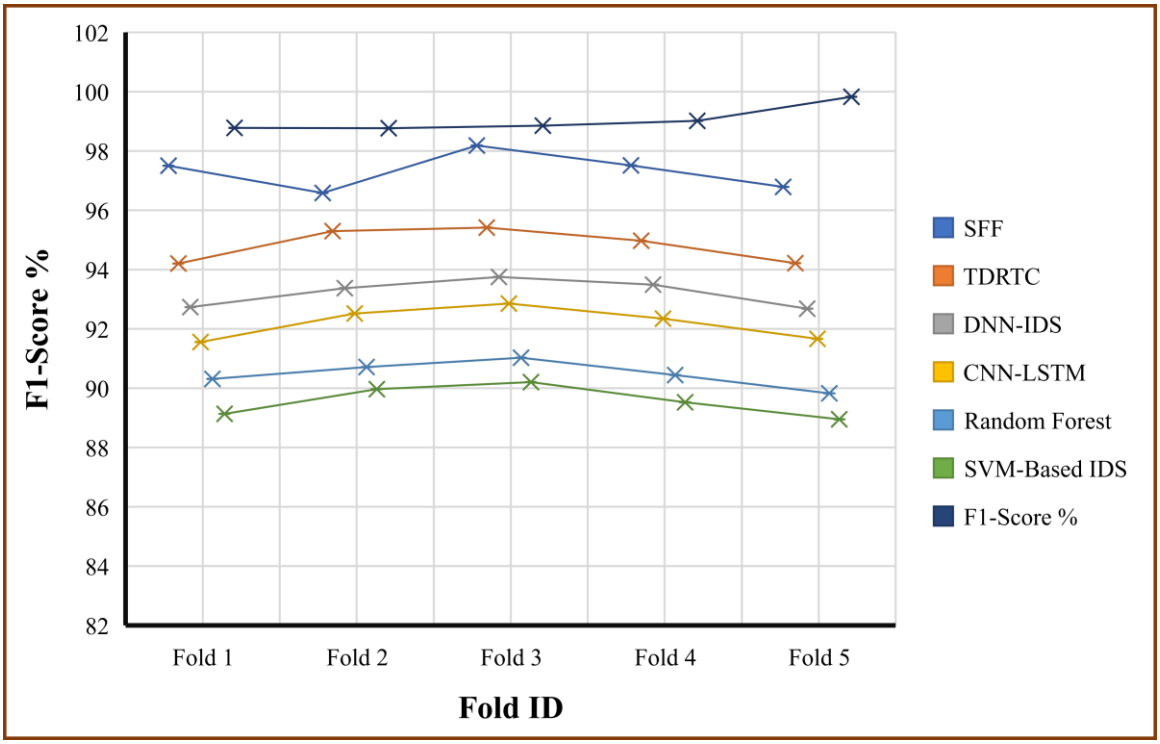

Figure 8. Graphical illustration of compared F1-Score

An assessment of F1-scores between the ID-ELC (Proposed) model and six intrusion detection approaches demonstrates consistent superiority of ID-ELC against existing methods across five folding iterations according to the provided table 5 and Figure 8. ID-ELC maintains a steady record of the highest F1-score across multiple experiments, which varied between 98.77% and 99.83% demonstrating its capability to strike a perfect equilibrium between precision and recall rates. F1-scores for SFF and TDRTC fall within 96.58% to 98.18% yet DNN-IDS, CNN-LSTM, Random Forest and SVM-Based IDS generate lower scores. ID-ELC demonstrates its effectiveness as an intrusion detection solution for IoT networks because it maintains a high F1-score through competent detection of malicious traffic and minimal occurrence of false positives and false negatives.

Table 6: Evaluation of compared MCC of existing approach with suggested approach

Method	**MCC**
SFF	0.9076
TDRTC	0.8227
DNN-IDS	0.8059
CNN-LSTM	0.7984
Random Forest	0.7803
SVM-Based IDS	0.7672
ID-ELC (Proposed)	0.9638

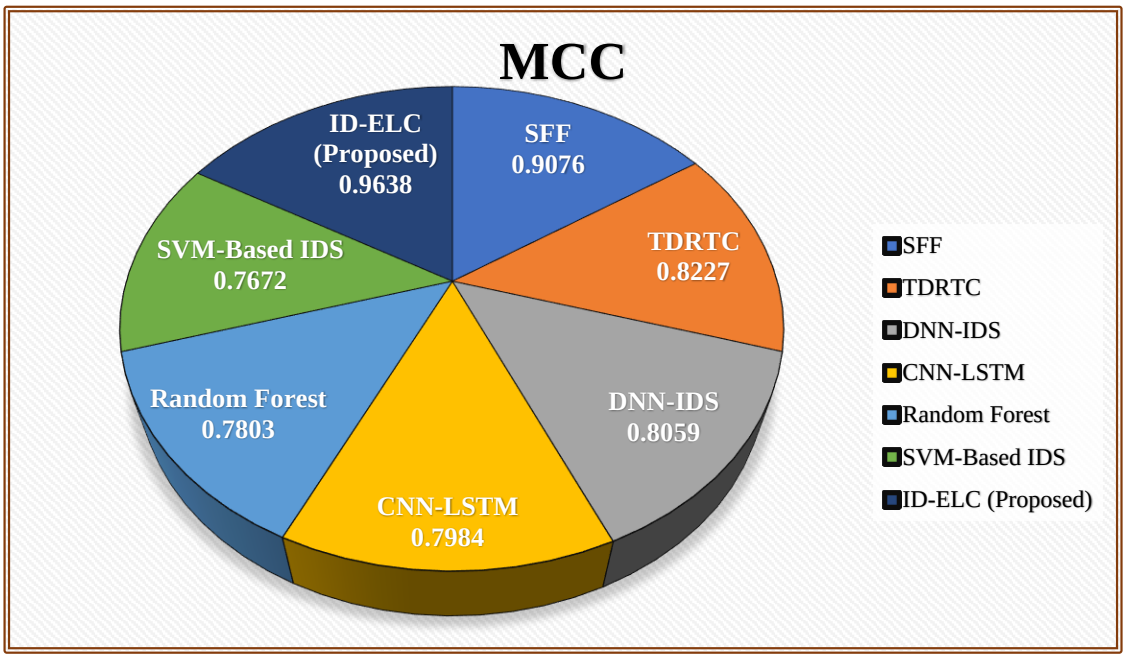

Figure 9. Graphical illustration of compared MCC

The table 6 and Figure 9 compares the Matthews Correlation Coefficient (MCC) of the ID-ELC (Proposed) model with six existing intrusion detection methods. ID-ELC demonstrates the best MCC rate of 0.9638, which stands above all other models tested. The Medium-level agreement exists between actual and predicted classifications where SFF and TDRTC reach 0.9076 and 0.8227 in correlation values. Nevertheless, DNN-IDS, CNN-LSTM, Random Forest and SVM-Based IDS exhibit lower correlation values indicating weaker predictive performance. The high Mathew Correlation Coefficient value of ID-ELC demonstrates its dependable nature and balanced performance and its ability to minimize false positives and false negatives that makes it a dependable system for IoT security intrusion detection.

7 Conclusion and Future Enhancement

This research work succeeds in developing Intrusion Detection by Ensemble Learning and Classification (ID-ELC) to enhance security for IoT networks through its improved intrusion detection framework. A proposed detection system achieves high accuracy and precision and recall values through its combination of Composite Variance and Cuckoo Search optimizations for feature selection features with ensemble classification methods. Research results show that ID-ELC delivers superior performance in detecting network intrusions than SFF and TDRTC as well as DNN-IDS and CNN-LSTM and Random Forest and SVM-Based IDS through measurements of Accuracy and Precision and Sensitivity (Recall), Specificity, F1-Score, and MCC across evaluation metrics. The model proves reliable in real situations because its Matthew Correlation Coefficient value stands at 0.9638. Between them, the ensemble approach creates enhanced detection classification capabilities, which decrease wrong outputs, and the hierarchical feature extraction process maximizes detection speed and performance. ID-ELC demonstrates scalability alongside high efficiency because it adapts to IoT environments effectively as a cybersecurity solution. The scientific contribution of this work enhances current intrusion detection methods to boost interconnected system security measures.

7.1 Future Enhancement

The research path should explore deep learning methods for ID-ELC to boost its feature extraction along with classification capabilities. The system requires expansion to identify zero-day attacks as well as real-time intrusion protection adaptations in edge and cloud platforms to provide greater IoT security. The deployment of ID-ELC in IoT devices that have limited processing power will be enhanced by optimizing computational efficiency.

References

[1] K. Wang, A. Zhang, H. Sun, and B. Wang, "Analysis of recent deep learning-based intrusion detection methods for in-vehicle network," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 1843–1854, Feb. 2023.

[2] A. Prasanth and S. Jayachitra, "A novel multi-objective optimization strategy for enhancing quality of service in IoT-enabled WSN applications," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 1905-1920, 2020.

[3] A. Smith, B. Johnson, and C. Lee, "A Machine Learning Approach for Cyber Threat Detection in IoT Environments," *Journal of Network and Computer Applications*, vol. 175, pp. 102900, Jan. 2023.

[4] C. Kalaiselvi and G. M. Nasira, "A new approach for diagnosis of diabetes and prediction of cancer using ANFIS," in *Proc. World Congress on Computing and Communication Technologies*, WCCCT 2014, pp. 188-190, 2014.

[5] M. Thiruvengadam et al., "Bioactive compounds in oxidative stress-mediated diseases: Targeting the nrf2/are signaling pathway and epigenetic regulation," *Antioxidants*, vol. 10, no. 12, pp. 1-12, 2021.

[6] M. Zakariah, S. A. AlQahtani, and M. S. Al-Rakhami, "Machine learning-based adaptive synthetic sampling technique for intrusion detection," *Applied Sciences*, vol. 13, no. 11, p. 6504, 2023.

[7] V. D. P. Jasti et al., "Computational technique based on machine learning and image processing for medical image analysis of breast cancer diagnosis," *Security and Communication Networks*, vol. 2022, pp. 1-12, 2022.

[8] V. Roy, L. Roy, R. Ahluwalia, G. Khambra, M. Ramesh, and K. Rajasekhar, "An advance implementation of machine learning techniques for the prediction of cervical cancer," in *Proc. 3rd IEEE Int. Conf. ICT in Business Industry and Government*, ICTBIG 2023, 2023.

[9] S. K. Suman et al., "Game theoretical approach for improving throughput capacity in wireless ad hoc networks," in *Proc. Int. Conf. Recent Trends in Information Technology*, ICRTIT 2014, pp. 10-12, 2014.

[10] H. K. Shakya et al., "Energy-proficient cluster enrichment in wireless sensor networks via categorized fuzzy clustering and multi-hop routing optimization," *SN Comput. Sci.*, vol. 6, no. 25, 2025.

[11] M. Alrizq et al., "Optimization of sensor node location utilizing artificial intelligence for mobile wireless sensor network," *Wireless Networks*, pp. 1-13, 2023.

[12] S. B. Sasi and N. Sivanandam, "A survey on cryptography using optimization algorithms in WSNs," *Indian Journal of Science and Technology*, vol. 8, no. 3, pp. 216-221, 2015.

[13] N. Dey et al., "Parameter optimization for local polynomial approximation based intersection confidence interval filter using genetic algorithm: An application for brain MRI image de-noising," *Journal of Imaging*, vol. 1, no. 1, pp. 60-84, 2015.

[14] V. A. Bhagyalakshmi et al., "Review of detecting diabetes mellitus and diabetic retinopathy using tongue images and its features," *Research Journal of Pharmaceutical Biological and Chemical Sciences*, vol. 8, no. 2, pp. 378-386, Apr. 2017.

[15] D. Musleh et al., "Intrusion detection system using feature extraction with machine learning algorithms in IoT," *J. Sensor Actuator Netw.*, vol. 12, no. 2, p. 29, Mar. 2023.

[16] L. Bhagyalakshmi et al., "Improving spectral efficiency and coverage capacity of 5G networks: A review," *Advances in Mathematics: Scientific Journal*, vol. 9, no. 6, pp. 3387-3397, 2020.

[17] A. Kashyap and J. Raghuvanshi, "A preliminary study on exploring the critical success factors for developing COVID-19 preventive strategy with an economy-centric approach," *Management Research: Journal of the Iberoamerican Academy of Management*, vol. 18, no. 4, pp. 357–377, Sep. 2020.

[18] G. Chauhan and V. Chauhan, "A phase-wise approach to implement lean manufacturing," *International Journal of Lean Six Sigma*, vol. 10, no. 1, pp. 106–122, Mar. 2019.

[19] P. K. Srivastava et al., "Internet of thing uses in materialistic ameliorate farming through AI," *AIP Conference Proceedings*, Jan. 2023.

[20] P. Shukla et al., "A wavelet features and machine learning founded error analysis of sound and trembling signal," *SN Computer Science*, vol. 4, 2023.

[21] N. Malik, “Authentic leadership – an antecedent for contextual performance of Indian nurses,” *Personnel Review*, vol. 47, no. 6, pp. 1244–1260, Sep. 2018.

[22] S. Kala et al., “Shadow and weak gravitational lensing of a rotating regular black hole in a non-minimally coupled Einstein-Yang-Mills theory in the presence of plasma,” *The European Physical Journal Plus*, vol. 137, no. 4, Apr. 2022.

[23] K. Sood et al., “Identification of Asymmetric DDoS Attacks at Layer 7 with Idle Hyperlink,” *ECS Transactions*, vol. 107, no. 1, pp. 2171–2181, Apr. 2022.

[24] C. Prabhu et al., “A novel approach to extend KM models with object knowledge model (OKM) and Kafka for big data and semantic web with greater semantics,” *Advances in Intelligent Systems and Computing*, pp. 544–554, Jun. 2019.

[25] Y. N. Prajapati and M. Sharma, “Designing AI to predict Covid-19 outcomes by gender,” Dec. 2023.

[26] Y. N. Prajapati and M. Sharma, “Novel machine learning algorithms for predicting COVID-19 clinical outcomes with gender analysis,” *Communications in Computer and Information Science*, pp. 296–310, Jan. 2024.

[27] J. A. Khan et al., “Diversity of antibiotic-resistant Shiga toxin-producing Escherichia coli serogroups in foodstuffs of animal origin in northern India,” *Journal of Food Safety*, vol. 38, no. 6, p. e12566, Oct. 2018.

[28] H. Gupta and C. Sharma, “Face mask detection using transfer learning and OpenCV in live videos,” in *Proc. 2022 Int. Conf. Fourth Industrial Revolution Based Technology and Practices*, ICFIRTP, pp. 115–119, Nov. 2022.

[29] V. Singh et al., “Big-Data Analytics,” pp. 275–291, Oct. 2022.

[30] A. Saini et al., “A proposed method of machine learning based framework for software product line testing,” Nov. 2022.

[31] H. Gupta et al., “A machine learning framework for detection of fake news,” *Communications in Computer and Information Science*, pp. 64–78, 2022.

[32] H. Jain and M. Mahadev, “An analysis of SMS spam detection using machine learning model,” in *Proc. 2022 Fifth Int. Conf. Computational Intelligence and Communication Technologies*, CCICT, Jul. 2022.