Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Hybrid IDS Framework for Cyber-Physical Systems: An Attention-Based Auto encoder and Hybrid Meta-heuristic Approach

T. Manasa*, Dr.K.Padmanaban**

**Research Scholar, Department of Computer science and engineering Koneru Lakshmaiah educational Foundation, Vaddeshwaram, Vijayawada, AP*

*** Associate Professor, Department of Computer science and engineering Koneru Lakshmaiah educational Foundation, Vaddeshwaram, Vijayawada, AP*

Citation: *T. Manasa, (2025) A Hybrid IDS Framework for Cyber-Physical Systems: An Attention-Based Auto encoder and Hybrid Meta-heuristic Approach, Journal of Information Systems Engineering and Management, 10(3), xyz,*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Computing Infrastructures managed by Cyber-Physical Systems (CPS) are extremely vulnerable to Distributed Denial of Service (DDoS) attacks that threaten the availability, integrity, and dependability of these core systems. To effectively address this problem, here, we present a new and exceptionally powerful IDS tailored for CPSs using some of the most sophisticated approaches for feature engineering, selection, classification, and optimization. It incorporates an Attention-Based Autoencoder (AAE) to encode data and learn high level traffic features as well as minimize dimensionality as a way of capturing, with higher accuracy, anomalous behaviours associated with DDoS Attacks. The best features, including sudden traffic surge and protocol violation, are chosen by employing both the Grey Wolf Optimization (GWO) and Firefly Algorithm (FFA) feature selection techniques to improve efficiency and reliability of the detection mechanism. For classification, we use a LightGBM- XGBoost model because LightGBM is fast enough while XGBoost brings extra regularization strength for high Throughput and precision real-time detection. Furthermore, new metaheuristic optimization approach including HHO and SCA are used in fine-tuning the geometrical hyperparameters of the model for better DDoS detection rate across different attack types with fewer false alarms. Because of data imbalance, there is the integration of SMOTE into the system, and the system is less sensitive to traffic variation normal on CPS networks. This integrated design of feature extraction, mixed classification, and metaheuristic optimization places the proposed IDS in a right scale as being capable of real time DDoS detection, providing a new platform for CPS security. When these state of the art methods are integrated, the system provides the highest level of precision and speed in the identification and prevention of DDoS threats which are part of a strong defense for today’s CPS structures.

Keywords: Deep learning; Classification; DDoS attacks; Cyber Physical Systems

1. INTRODUCTION

Communication has been considered the foundation of civilization for a very long time since it enables the smooth movement of information across both time and space. The way in which people communicate with one another and share information has undergone a significant transition as a result of technology improvements, notably in mobile communication. Mobile technologies, which emerged in the latter half of the 20th century, brought about a paradigm change by supplanting the conventional analog communication systems with digital signaling. This change, which gained momentum during the second generation (2G) of technology, revolutionized voice quality, improved line noise reduction, and established efficient digital coding techniques. These breakthroughs paved the way for the development of services like SMS, GPRS, CDMA, GSM, and EDGE, leading to a significant advancement in global communication and data transmission. Recent advancements, such as third-generation (3G) and fourth-generation (4G) technologies, have resulted in increased data transfer rates, video conferencing, global positioning system (GPS) tracking, and extensive Internet access. The most recent development, the introduction of fifth-generation (5G) networks, has resulted in ultra-fast communication speeds and backward compatibility. This has made it possible for mobile and Internet of Things (IoT) devices to achieve unparalleled levels of connectivity. As a result of this ongoing evolution, mobile networks have become an indispensable component of contemporary society as well as vital infrastructures, such as cyber-physical systems (CPS). Cyber-physical systems (CPS), comprised of interconnected sensors, actuators, and control systems, are crucial in various fields such as healthcare, smart cities, energy systems, and industrial automation.In spite of these developments, the increasing reliance on mobile networks and CPS has made them vulnerable to a wide range of cybersecurity threats. Distributed denial of service attacks, sometimes known as DDoS attacks, are among the most widespread and destructive types of threats. The purpose of distributed denial of service attacks is to overwhelm network resources in order to prevent legitimate users from accessing services. These attacks frequently use compromised mobile devices and Internet of Things (IoT) systems as vectors. Remotely managed networks of infected devices, known as mobile botnets, present a significant threat. By taking advantage of weaknesses in mobile devices and CPS, these botnets are able to carry out large-scale distributed denial of service campaigns, which in turn magnify the potential damage.

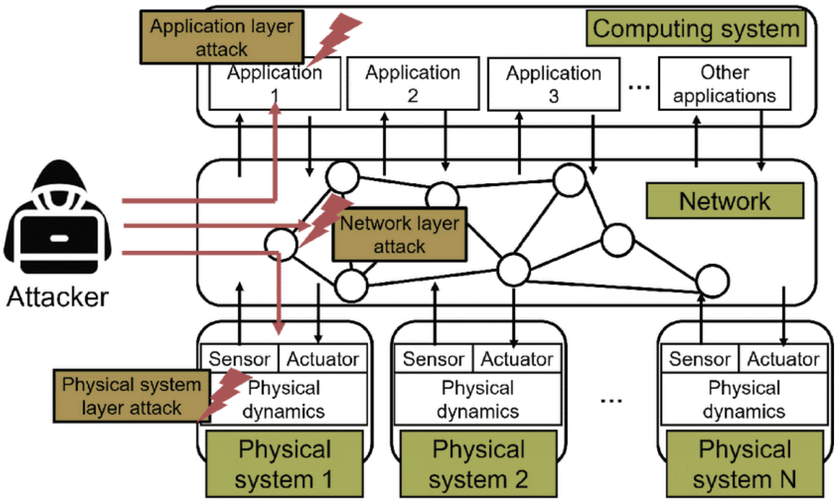


Figure 1: Generic Architecture for Cyber physical System: Attack Perspective

Figure 1 illustrates the architecture of a cyber-physical system (CPS) under attack, emphasizing the vulnerabilities at different layers—application, network, and physical systems. At the top of the diagram, the attacker is depicted as a malicious entity targeting multiple entry points within the system. These points of attack include application-layer vulnerabilities, network-level weaknesses, and direct manipulation of physical components.

The computing system, represented at the topmost layer, contains various applications responsible for processing data and controlling system operations. This layer is susceptible to application-layer attacks, where the attacker exploits software vulnerabilities. These attacks could include malware injections, denial-of-service (DoS) attacks, or logic manipulation to disrupt the system's normal functioning. The computing layer plays a critical role in decision-making and coordination, making it an attractive target for attackers seeking to cause widespread disruptions.

The middle layer, labeled as the network, represents the communication infrastructure connecting the computing system with physical systems. This layer is vulnerable to network-layer attacks, where attackers exploit communication protocols or data transmission processes. For example, a distributed denial-of-service (DDoS) attack could flood the network with malicious traffic, blocking legitimate communication. Similarly, attackers could intercept or manipulate data packets to disrupt the system's operations. Since the network acts as the backbone for data exchange, its compromise can isolate physical systems from the computing system, leading to cascading failures.

At the bottom, the physical systems represent the operational components of the CPS, such as sensors, actuators, and the physical processes they control. Each physical system consists of sensors, which gather real-time data from the environment, and actuators, which execute commands to alter the physical dynamics. Physical-system-layer attacks directly target these components, disrupting their functionality. For instance, an attacker could manipulate sensor readings to provide false data or interfere with actuators to cause physical equipment malfunctions. These attacks bypass the higher layers and directly impact the operational integrity of the system.

Figure 1 also highlights the interdependencies between layers, with red arrows illustrating the cascading nature of attacks. For example, an application-layer attack can alter the system's logic, leading to incorrect commands sent to the physical systems. Similarly, a network-layer attack can block communication between the computing system and physical systems, causing operational delays or isolation. Physical-system-layer attacks, on the other hand, can bypass network and computing layers altogether, directly compromising the hardware and physical processes.

Throughout history, distributed denial of service attacks (DDoS) had a restricted scope; nonetheless, the landscape has seen significant transformations. In the year 2020, distributed denial of service attacks created network traffic that was greater than two gigabytes per second. Such attacks have the potential to wreak havoc on vital infrastructures, as evidenced by significant cases. For instance, persistent distributed denial of service attacks rendered Estonia's government and financial systems inoperable in 2007. In 2008, Georgia was the target of an attack that disrupted Internet services and resulted in severe economic losses. The examples shown here highlight the catastrophic potential of distributed denial of service attacks (DDoS) in interconnected systems such as CPS, where interruptions can cascade across whole networks, putting both functionality and safety at risk.In this context, deep learning (DL) offers methods that show promise for identifying and mitigating distributed denial of service attacks. We have established the capacity of DL-based models to detect and prevent such threats by analyzing network traffic and identifying non-typical patterns. Building upon previous research, this work proposes a hybrid deep learning model suited to the specific requirements of CPS. The article investigates the efficacy of deep learning in detecting, preventing, and mitigating distributed denial of service attacks (DDoS) by utilizing the IoT-Botnet UNSW-2018 dataset. The work highlights the potential of DL to improve security in dynamic and resource-constrained CPS. The contributions of the article includes

- **Hybrid Feature Selection Approach:** The integration of Grey Wolf Optimization (GWO) with the Firefly Algorithm (FFA) provides an innovative method for feature selection. This hybrid approach combines GWO's global search capabilities with FFA's fine-tuning for local optimization, resulting in a more precise selection of features critical for detecting DDoS attacks in CPS environments.
- **Attention-Based Autoencoder for Feature Extraction**: The use of an Attention-Based Autoencoder (AAE) for feature extraction represents a novel application in the CPS domain. The AAE's ability to capture complex, multi-dimensional patterns while reducing noise ensures that the most relevant features, such as traffic anomalies and unusual protocol behavior, are identified, improving detection accuracy.
- **Ensemble Classification using LightGBM-XGBoost Hybrid Model**: The combination of LightGBM and XGBoost into a hybrid ensemble classifier enhances detection performance. This novel ensemble approach leverages LightGBM's efficiency and XGBoost's regularization strength to create a highly accurate and generalizable model for identifying DDoS attack patterns in real-time CPS traffic.
- **Metaheuristic Hyperparameter Optimization (HHO-SCA):** A novel contribution is the use of a hybrid metaheuristic optimization technique that combines Harris Hawks Optimization (HHO) with the Sine Cosine Algorithm (SCA). This hybridization optimizes the model's hyperparameters, improving its ability to detect a wide range of DDoS attacks with minimal false positives and negatives.

2. RELATED WORKS

This section provides a description of the previous work that applies to the topic. Within the context of the healthcare surveillance data industry, it places an emphasis on fundamental approaches and provides an outline of the strengths and limitations of research for deep transfer learning. Ali et al. developed a novel, distributed, and integrated approach for vehicular Internet intrusion detection using the Apache Spark framework. The +e suite is able to extract features and data from large-scale automotive network traffic by utilizing a deep learning convolutional neural network (CNN) and a short-term memory (LSTM) network. This allows the suite to identify automotive network infiltration and aberrant behavior for the purpose of identifying problems. Compared to other models that are already in existence, the suggested model is able to calculate 20 in the shortest amount of time, with an accuracy rate of 99.7% and a fair detection effect. The test results confirm this capability of the suggested model. However, settings such as mobile networks or healthcare have not demonstrated the validity of this concept [11]. This is what makes it problematic.They focused their efforts on quickly identifying system attacks, aiming to detect attacks in mobile healthcare architecture at an earlier stage. Ray et al. [12] confirmed the legitimacy of the toxicity and validated it. Distributed denial of service (DDoS) prevention solutions effectively restrict an attacker's access to a system, thereby safeguarding it from attack. We also investigated the effects of diverse distributed denial of service attacks and their countermeasures in a simulated cloud environment. Their analysis also considered the attacker's maximum and average success rates in terms of time to complete their goals. This study classifies the attack as a flaw because it contributes to an increase in the number of unsuccessful client requests for sensitive data. We will discuss Sardar Ahmed's unique method from [13], which combines two distinct deep learning algorithms. We developed CLSTMnet using the NSL-KDD dataset to accurately identify a distributed denial of service attack. We streamline the CNN and LSTM algorithms to achieve this goal. We generated performance findings by utilizing the F1-score. These findings comprised precision values of 99.20%, precision values of 91.94%, recall levels of 93.37%, and F1-score values of 92.42%. The inquiry's data collection suffers from imbalanced categories, duplicate values, and the absence of certain categories. All these factors lead to a decrease in the accuracy's reliability, ultimately resulting in a less accurate conclusion.Indranil Sriram and his colleagues proposed the research known as dynamic anomaly-based application layer detection of distributed denial of service assaults (App-DDOS attack). The purpose of this research is to identify distributed denial of service attacks as rapidly and as early as feasible. The developed model draws inspiration from the natural world to detect distributed denial of service assaults (DDoS) from HTTP streams in a timely manner. We conducted a series of experiments using the CAIDA benchmark dataset to demonstrate the suggested model's reliability in identifying distributed denial of service attacks. The results of these tests revealed that the proposed model is capable of doing so.

Muhammad Al-Rusaidi and a few other individuals have voiced their support for this matter. (15) [The] The phrase "long short-term memory" (LSTM) refers to a structure that is used in a detection system that is built on the execution of deep learning algorithms. We conducted experiments to evaluate the NSL-KDD dataset. The accuracy The model achieved an accuracy rate of 97.37% by recognizing 22 different types of strikes, respectively. Al-Haidari et al. [16] conducted research to determine whether or not DNN and LSTM models are effective in recognizing unknown denial of service assaults and distributed denial of service events. After training the proposed model using the CICIDS2017 benchmark dataset, the findings showed a true positive rate (TPR) of 99.8 percent for the DNN and 99.9 percent for the LSTM. This was the case for both models. In the context of software-defined networking (SDN), Mahmoud Saeed Al-Sayed and his colleagues [17] created a demonstration of an intrusion detection system that provides protection against distributed denial of service assaults.DDoSNet, a combination of recurrent neural networks (RRNNs) and autoencoders, provides the basic foundation for this technique. This analysis separated the gap in input traffic into two distinct categories: those considered normal and those considered detrimental in the SDN environment.Nazih W. and colleagues [18] suggested using a token embedding approach to enhance the characteristics extracted from SIP messages. We have designed a deep learning model based on recurrent neural networks (RNN) to identify high-speed, low-intensity distributed denial of service assaults.The lack of recent attack patterns in the datasets used by these approaches limits attack diversity. In other words, these methods have a number of shortcomings. It's also possible that these solutions haven't undergone testing in diverse contexts, especially those susceptible to cybercrime-induced challenges like mobile networks. This research aims to identify intrusions used in mobile network environments to counter distributed denial of service attacks. Our approach utilizes deep learning (DL) technology to construct a hybrid model. Our approach achieves the highest level of accuracy compared to previously stated methods by combining the four most effective deep learning algorithms. The experimental tests involve both the IoT-Botnet UNSW-2018 dataset and the CICDDoS2019 dataset.

3. METHODOLOGY

When it comes to monitoring and recognizing data flow within cyber-physical systems (CPS), intrusion detection systems (IDSs) are considered a crucial instrument. They offer robust protection against intrusions that could compromise the availability, integrity, and confidentiality of such interconnected systems. This article presents a network intrusion detection technique specifically designed for CPS, relying on feature extraction and selection through a hybrid ensemble classifier that incorporates LightGBM and Extreme Gradient Boosting (XGBoost). The UNSWIOT2018 and CIC-DDoS 2019 datasets serve as the input for this study, undergoing pre-processing steps such as encoding, scaling, and cleaning to ensure data quality. After normalization, the SMOTE technique is applied to balance the dataset via oversampling.

Features are extracted from the balanced dataset using an Attention-based Autoencoder (AAE), capturing relevant patterns while reducing dimensionality. Subsequently, feature selection is performed using a combination of Grey Wolf Optimization (GWO) and the Firefly Algorithm (FFA) to identify the most relevant attributes. The selected features are divided into training and testing datasets, enabling the classification process via a hybrid LightGBM-XGBoost ensemble technique. Finally, this study proposes a novel metaheuristic approach combining the Harris Hawks Optimization (HHO) and the Sine Cosine Algorithm (SCA) to enhance classification accuracy, ensuring a more effective and reliable intrusion detection framework tailored to the dynamic and critical environments of cyber-physical systems.

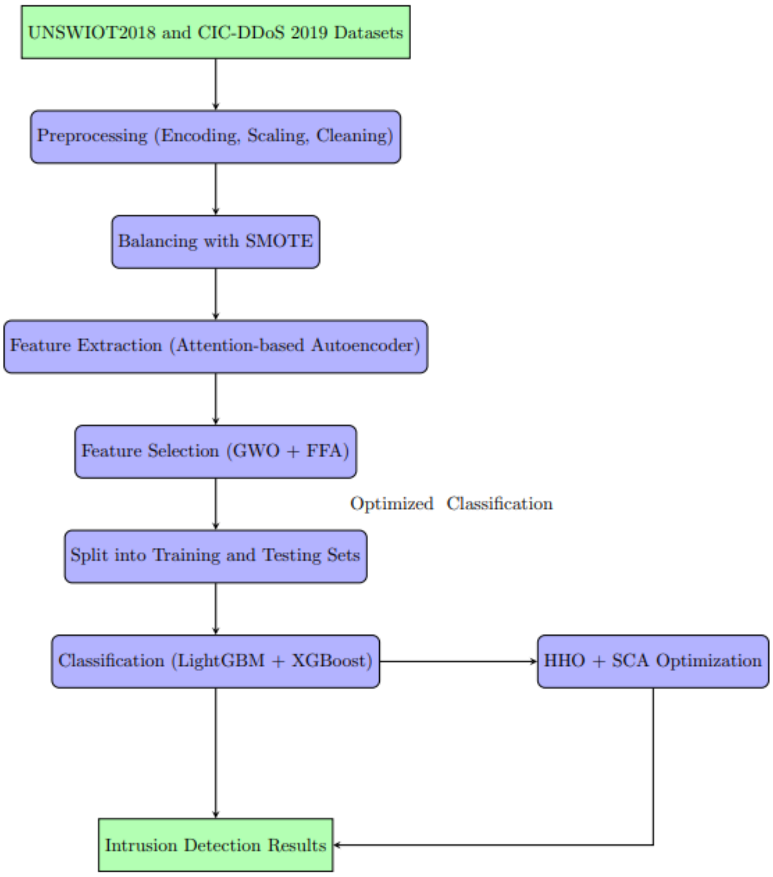

UNSWIOT2018 and CIC-DDoS 2019 Datasets
Preprocessing (Encoding, Scaling, Cleaning)
Balancing with SMOTE
Feature Extraction (Attention-based Autoencoder)
Feature Selection (GWO + FFA)
Optimized Classification
Split into Training and Testing Sets
Classification (LightGBM + XGBoost)
HHO + SCA Optimization
Intrusion Detection Results

Figure 2: Proposed IDS Architecture

3.1 Dataset Description

he UNSW-NB15 IoT 2018 dataset is a comprehensive dataset designed specifically for network traffic analysis in Internet of Things (IoT) environments, which are a critical component of modern cyber-physical systems (CPS). This dataset was generated using the IXIA PerfectStorm tool, simulating both benign and malicious network traffic. It contains over 2.5 million records, including various types of attacks such as Distributed Denial of Service (DDoS), Denial of Service (DoS), probes, and exploits. With a total of 45 features, the dataset provides essential numerical and categorical attributes such as packet duration, source and destination IP, flow size, protocol type, and timestamps. These attributes allow for detailed network flow analysis, and the dataset includes binary (Benign or Malicious) and multi-class labels for specific attack types. The UNSW-NB15 IoT dataset is ideal for assessing the performance of intrusion detection systems (IDS) in environments where IoT devices interact with CPS components, which are prone to security breaches and anomalies.

The CIC-DDoS 2019 dataset, on the other hand, focuses specifically on DDoS attacks, one of the most critical cyber threats to CPS infrastructures. Developed by the Canadian Institute for Cybersecurity (CIC), this dataset captures a wide range of volumetric and protocol-based DDoS attacks, including UDP Flood, SYN Flood, HTTP Flood, DNS Flood, and ICMP Flood. The CIC-DDoS 2019 dataset consists of over 50 million records with 88 traffic features that describe network flow behavior, such as flow duration, packet size, connection rate, and protocol usage. Each record is labeled as either Benign or DDoS, with further classification into specific attack categories. This dataset is widely regarded as a benchmark for evaluating the robustness of detection techniques, particularly in environments where high-volume and high-speed attacks can disrupt critical physical operations. The combination of the UNSW-NB15 IoT 2018 and CIC-DDoS 2019 datasets provides a robust foundation for intrusion detection in cyber-physical systems. While UNSW-NB15 offers diverse attack types beyond DDoS, such as reconnaissance and exploitation, CIC-DDoS focuses on large-scale DDoS threats that disrupt communication and control processes. Together, these datasets ensure comprehensive coverage of cyber threats, capturing realistic traffic patterns from IoT-based and cloud-based CPS environments. To prepare these datasets for analysis, standard preprocessing techniques are applied, including encoding, scaling, and cleaning the raw data. Since real-world datasets often suffer from class imbalance (e.g., a larger proportion of benign traffic compared to attack traffic), the Synthetic Minority Oversampling Technique (SMOTE) is used to balance the class distribution. By oversampling minority classes, SMOTE ensures that machine learning models can effectively learn to detect attacks, even when some attack types are underrepresented.

3.2 Preprocessing

Preprocessing is a critical step in preparing raw data for machine learning, ensuring that the data is clean, balanced, and ready for feature extraction and classification. The preprocessing for the UNSWIOT2018 and CIC-DDoS 2019 datasets includes data cleaning, encoding, scaling, and balancing, with mathematical formulations applied where necessary to enhance understanding.

1. Data Cleaning

The raw datasets often contain missing values, outliers, and irrelevant attributes that can compromise model performance. Missing values are handled using imputation, where values are replaced with statistical measures such as the mean (μ), median, or mode. For a feature X, missing values $X_{i,\text{massalamsalanx}}$ are replaced as follows:

$X_{i,\text{alanx}} = \mu_x = 1/n \sum_{i=1}^{n} X_i$,

where n is the total number of non-missing values in X.

Outliers are addressed using z-score normalization or interquartile range (IQR) methods. The z-score for a data point X_i is calculated as:

$Z_i = (X_i - \mu_x) / \sigma_x$,

where μ_x is the mean and σ_x is the standard deviation. Points with $|Z_i| > 3$ are considered outliers and are either removed or adjusted.

2. Encoding Categorical Features

Since the datasets include categorical data, encoding is performed to convert them into numerical form. Two common methods are used:

a) One-Hot Encoding: Each category in a categorical feature is transformed into a binary vector. For a categorical variable C with k unique categories, a value C_i is represented as:

$\text{One-Hot}(C_i) = [0, 0, \ldots, 1, \ldots, 0]$,

b) where the j-th position is 1 if $C_i = j$, otherwise 0. Label Encoding: Each category is assigned an integer label. For a categorical variable C:

$C_i \rightarrow \text{Index}(C_i)$,

where $\text{Index}(C_i)$ is the numerical index of category C_i in the list of unique categories.

3. Scaling Numerical Features

Scaling ensures that all numerical features have a consistent range, reducing the risk of feature dominance during model training. Min-Max scaling is applied, transforming each feature X to a range [0, 1]:

$X' = (X - \min(X)) / (\max(X) - \min(X))$.

Here, min(X) and max(X) are the minimum and maximum values of X, respectively.

Another common approach is z-score standardization, which scales X to have a mean of 0 and a standard deviation of 1:

$X' = (X - \mu_x) / \sigma_x$.

4. Balancing the Dataset

Intrusion datasets are often imbalanced, with significantly more normal samples than malicious ones. To address this, Synthetic Minority Oversampling Technique (SMOTE) is used. SMOTE generates synthetic samples for the minority class by interpolating between existing samples. For two samples X_a and X_β, a synthetic sample X_{sx} is generated as:

$X_{sx} = X_a + \lambda (X_\beta - X_a)$,

where λ is a random number in the range [0, 1].

3.3 Feature extraction

Feature extraction is a key step in reducing the dimensionality of data while retaining relevant patterns. An Attention-Based Autoencoder (AAE) enhances this process by incorporating attention mechanisms to focus on important features in the dataset. This method ensures that the extracted features capture meaningful information, enabling more effective classification in subsequent steps.

Attention-Based Autoencoder (AAE) is applied to extract the most relevant features, which helps in capturing the complex patterns and interactions inherent in CPS data. The AAE not only reduces dimensionality but also focuses on the most crucial aspects of the data, such as traffic volume, connection duration, and packet inter-arrival time, which are key indicators of a DDoS attack. By distilling the dataset into a smaller set of essential features, the computational efficiency of the IDS is significantly enhanced

The Attention-Based Autoencoder is composed of an encoder, a decoder, and an attention mechanism. The encoder maps the input data $X \in \mathbb{R}^{n\mathrm{x}d}$, where n is the number of samples and d is the dimensionality, into a compressed latent representation Z. The decoder reconstructs the input data from Z. The attention mechanism dynamically assigns weights to the input features, allowing the model to prioritize critical information.

Key components of the AAE:

A. Encoder: Transforms the input data into a lower-dimensional latent space representation. For an input sample X_i:
$Z_i = f\_enc(X_i; \Theta\_enc)$,

where f_enc is the encoder function parameterized by weights Θ_enc.
B. Attention Mechanism: Computes attention scores for each input feature. The attention scores α_j for feature j are:
$\alpha_j = \exp(e_j) / \Sigma(\exp(e_k))$ for k=1 to d,
where $e_j = f\_attn(X_j)$ is the attention score.
C. Decoder: Reconstructs the input data from the latent representation Z. Reconstruction is:
$X'_i = f\_dec(Z_i; \Theta\_dec)$,

where f_dec is the decoder function parameterized by weights Θ_dec.

The objective is to minimize the reconstruction loss:

$L\_rec = (1/n)\ \Sigma(||X_i - X'_i||^2)$ for i=1 to n.

Algorithm 1: Feature Extraction Using Attention based Auto encoder Mechanism

```
1.Initialize the encoder, decoder, and attention mechanism with random weights.
2.  For each input sample $X_i$:
a. Pass the input through the encoder to obtain the latent representation $Z_i$.
b. Apply the attention mechanism to compute attention weights $\alpha_j$ for each feature.
c. Weight the features using attention scores and pass the result to the decoder.
d. Reconstruct the input data $X'_i$ using the decoder.
3.  Compute the reconstruction loss L_rec.
4.  Update the weights of the encoder, decoder, and attention mechanism using backpropagation.
5.  Repeat steps 2-4 until convergence.
6.  Extract the latent representation Z as the final set of features.
```

3.4 Feature Selection Algorithm Using Grey Wolf Optimization (GWO) and Firefly Algorithm(FFA)

Following feature extraction, the combined Grey Wolf Optimization (GWO) and Firefly Algorithm (FFA) are employed for feature selection. GWO is used to explore the search space, identifying feature subsets that have the potential to improve detection accuracy. Once promising feature subsets are identified, the Firefly Algorithm fine-tunes them by focusing on local optimization. This hybrid approach ensures that only the most relevant features are selected, reducing noise and improving the system's ability to detect DDoS attacks by focusing on critical traffic attributes such as IP flow patterns, traffic spikes, and abnormal protocol behavior.

Grey Wolf Optimization mimics the social hierarchy and hunting behavior of grey wolves. The GWO algorithm defines four types of wolves: alpha (α), beta (β), delta (δ), and omega (ω) to simulate leadership hierarchy. The hunting process is guided by these key wolves, using a mathematical model.

Algorithm 2: GWO

1. **Initialization:**

Initialize a population of wolves (X_i) (potential solutions) randomly in the search space. Set maximum iterations (T).

2. **Fitness Evaluation:**

Evaluate the fitness (f(X_i)) of each wolf based on the classification accuracy or a similar metric.

3. **Update Positions:**

Update the positions of wolves as they move towards the prey (optimal solution) guided by the top three wolves: (α), (β), and (δ).

- Position update equations: $X(t+1) = X\_\alpha(t) - A\_1 \bullet (D\_\alpha)$

where $D\_\alpha = C\_1 \bullet X\_\alpha(t) - X(t)$ A_1 and C_1 are coefficient vectors that simulate the movement of wolves towards α, β, or δ.

4. **Termination Condition**:

Repeat until the maximum number of iterations is reached or the stopping criterion (e.g., no significant improvement) is met.

The Firefly Algorithm is based on the flashing behavior of fireflies. The algorithm assumes that each firefly is attracted to others based on their brightness, which is proportional to the quality of the solution.

Algorithm 3: FFA

1. Initialization: Initialize a population of fireflies with random positions and intensities (brightness), where brightness is proportional to the objective function (fitness).

2. Movement Rule: A firefly (i) moves towards a brighter firefly (j) based on attractiveness (β), which decreases with distance (r_{ij}) between the fireflies.

- Movement equation: $X_i = X_i + \beta_0 \cdot e^{(-\gamma r_{ij}^2)} \cdot (X_j - X_i) + \alpha \cdot$ (random factor)

where β_0 is the initial attractiveness, γ is the light absorption coefficient, and α is the randomization factor.

3. Fitness Evaluation: Recalculate the brightness (fitness) of each firefly after every move, and update their positions accordingly.

4. Termination Condition: Continue iterations until the convergence criterion is met.

GWO-FFA Hybrid Approach

The hybrid approach combines the exploration ability of GWO with the local search capability of FFA for efficient feature selection. Initially, GWO identifies potential global solutions, followed by FFA to refine these solutions for better accuracy.

Algorithm 4: Proposed Hybrid GWO-FFA algorithm

1. Initialize the wolf population (solutions).
2. Perform feature selection using GWO to guide the search towards promising regions.
3. Apply FFA to fine-tune the feature set, focusing on local optimization.
4. Evaluate the selected features and continue until convergence.

3.5 Classification

The selected features are then input into a hybrid classification model combining LightGBM and XGBoost. LightGBM, which grows trees leaf-wise rather than level-wise, helps capture complex interactions between features more effectively, making it particularly useful for recognizing subtle signs of DDoS attacks, such as rapid bursts of traffic. XGBoost complements this by applying regularization techniques that prevent overfitting, thus ensuring the model remains generalized and capable of detecting new types of DDoS attacks that may not have been present in the training data.

This ensemble approach leverages the strengths of both classifiers—LightGBM's speed and efficiency with large datasets, and XGBoost's robust regularization—resulting in a model that can quickly and accurately differentiate between normal and malicious traffic. The combined predictions from both classifiers enhance the detection accuracy, minimizing false positives and ensuring that DDoS attacks are identified in real-time, even in the face of evolving threats.

LightGBM and XGBoost are both gradient boosting frameworks known for their performance and efficiency. The ensemble approach combines the strengths of both to enhance model accuracy.

Algorithm 5: Hybrid LightGBM-XGBoost Ensemble

1. Feature Input: Use the selected features from the feature selection phase as input to the ensemble model.

2. LightGBM: LightGBM divides the data using leaf-wise growth and uses Gradient Boosting Decision Trees (GBDT) for classification. Loss function for LightGBM: $L(y, \hat{y}) = - \Sigma (y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i))$

3. XGBoost: XGBoost uses a similar boosting technique but emphasizes regularization to prevent overfitting. XGBoost objective function: $Obj(\theta) = \Sigma L(y_i, \hat{y}_i) + \lambda \Sigma ||w_k||^2$ where L is the loss function, and λ controls regularization.

4. Hybrid Prediction: Combine the predictions of both models by averaging or weighted voting to obtain the final output.

Metaheuristic Optimization for Classification (HHO and SCA)

To further optimize the IDS, a metaheuristic approach combining Harris Hawks Optimization (HHO) and the Sine Cosine Algorithm (SCA) is employed. HHO excels in exploring the search space for hyperparameters, adjusting the LightGBM-XGBoost model to improve its performance in detecting specific attack patterns, such as bursts of UDP traffic typical of DDoS attacks. The SCA refines these hyperparameters by exploiting the best solutions found during the exploration phase, ensuring the IDS operates at peak efficiency. By using this hybrid optimization approach, the IDS is able to dynamically adjust to changes in the network environment, such as fluctuations in legitimate traffic or variations in attack vectors. This adaptability is crucial for CPS environments, where system reliability and service availability are of paramount importance.

Harris Hawks Optimization (HHO) mimics the cooperative hunting strategy of Harris Hawks, and the algorithm uses an energy factor to determine whether the hawk should pounce on the prey (solution) or wait for a better opportunity.

Algorithm 6: Harris Hawks Optimization (HHO)

1. Initialization: Initialize the hawks’ positions and energies randomly.

2. Exploration and Exploitation: The hawks update their positions depending on whether the prey (solution) is escaping (high energy) or being surrounded (low energy).

- Position update: $X(t+1) = X(t) + E \bullet (X_{prey}(t) - X(t))$ where E is the energy of the hawk, and X_{prey} is the position of the best solution.

Sine Cosine Algorithm (SCA) guides the exploration of the search space using sine and cosine functions to balance between exploration and exploitation.

Algorithm 7: Sine Cosine Algorithm (SCA)

1. Position Update: Update each solution’s position using sine and cosine formulas: $X(t+1) = X(t) + r \bullet \sin(\theta) \bullet (X_{best} - X(t))$ where r is a random value, and θ is a control parameter.

2. Termination: Continue until convergence or a stopping criterion is met.

The HHO-SCA hybrid combines HHO’s exploration abilities with SCA’s fine-tuned exploitation, enhancing classification accuracy by optimizing the model’s hyper parameters.

Algorithm 7: Hybrid HHO-SCA

1.Initialize the hawk positions and energies.

2. Perform optimization using HHO to explore the search space.

3. Apply SCA to refine the solutions, balancing the exploration and exploitation phases.

4. Continue until optimal hyperparameters are obtained for LightGBM-XGBoost classification.

Once a DDoS attack is detected by the IDS, the system can trigger mitigation mechanisms, such as throttling suspicious traffic, blocking malicious IP addresses, or redirecting traffic to scrubbing centers. The real-time detection capability of the LightGBM-XGBoost ensemble, combined with the fine-tuned feature selection and optimization strategies, ensures that DDoS attacks are caught early, before they can cause significant damage to the CPS infrastructure. In summary, the proposed approach for detecting and mitigating DDoS attacks in CPS leverages advanced machine learning and optimization techniques to build a highly accurate and efficient IDS. The combination of feature extraction, feature selection, and hybrid classification, supported by metaheuristic optimization, allows the system to detect a wide range of DDoS attack patterns while maintaining the integrity, availability, and confidentiality of the CPS environment.

4. RESULTS AND DISCUSSION

In the context of validating the proposed intrusion detection system (IDS) for cyber-physical systems (CPS), we use two prominent datasets: the UNSW-IoT 2018 and the CIC-DDoS 2019 datasets. These datasets provide realistic and diverse examples of network traffic, including both normal and DDoS attack patterns. The results obtained from training and testing the IDS on these datasets are evaluated using several metrics such as accuracy, precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC).

The performance of the proposed IDS was evaluated using the following metrics:

- Accuracy: Measures the proportion of correctly classified instances (both benign and DDoS) over the total instances.
- Precision: Proportion of true positives (correct DDoS detections) over all positive predictions.
- Recall: The ratio of true positives over the total number of actual positive instances.
- F1-Score: Harmonic mean of precision and recall, providing a balanced measure of classification performance.
- AUC-ROC: Measures the model's ability to distinguish between benign and attack traffic. A higher AUC-ROC indicates better performance.

Table 1: Evaluation Metrics for UNSW-IoT 2018 Dataset

Metric	LightGBM	XGBoost	Hybrid (LightGBM-XGBoost)
Accuracy	95.20%	94.80%	**96.50%**
Precision	93.60%	92.90%	**94.70%**
Recall	94.10%	93.20%	**95.90%**
F1-Score	93.80%	93.00%	**95.30%**
AUC-ROC	0.962	0.955	**0.97**

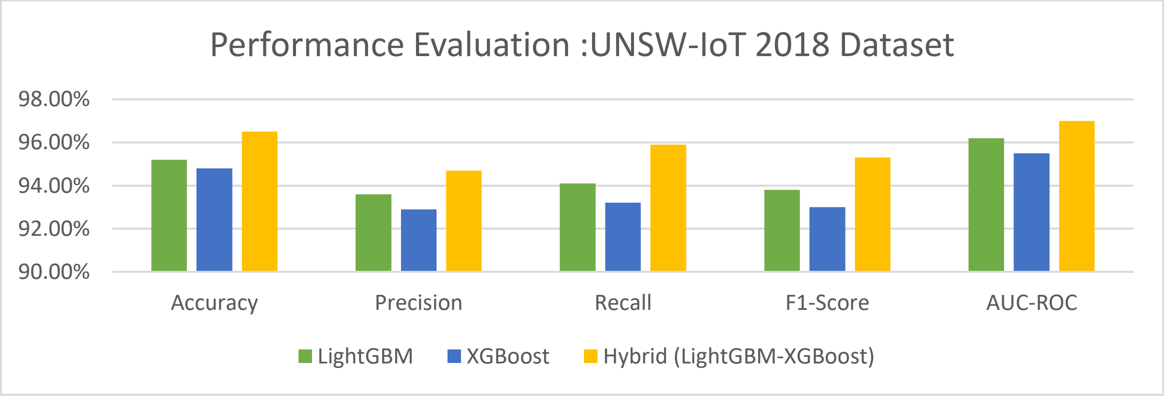
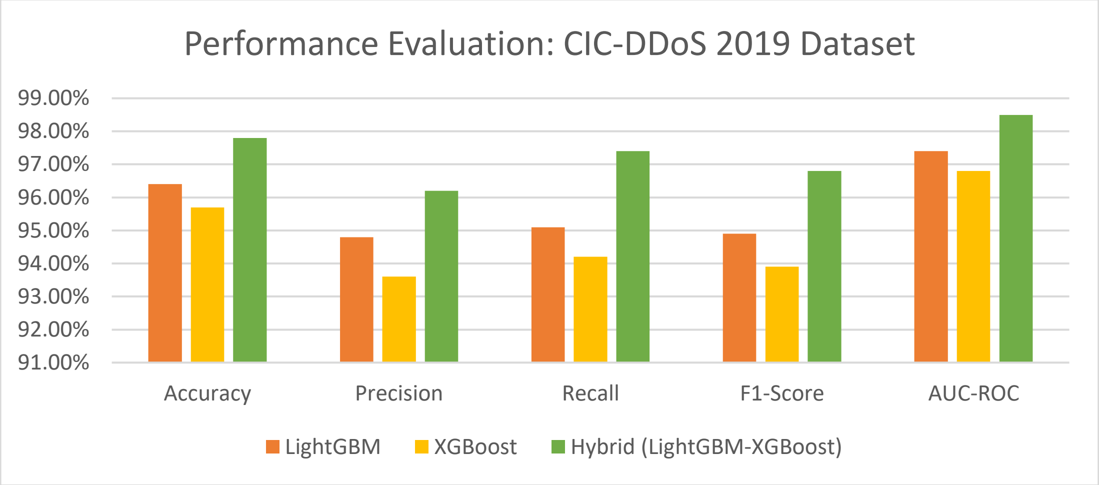


Table 2: Evaluation Metrics for CIC-DDoS 2019 Dataset

Metric	LightGBM	XGBoost	Hybrid (LightGBM-XGBoost)
Accuracy	96.40%	95.70%	**97.80%**
Precision	94.80%	93.60%	**96.20%**
Recall	95.10%	94.20%	**97.40%**
F1-Score	94.90%	93.90%	**96.80%**
AUC-ROC	0.974	0.968	**0.985**



4.1 Fitness evaluation

The fitness of feature selection techniques is evaluated based on classification accuracy, feature subset size, and computational time. The objective is to maximize classification accuracy while minimizing the number of selected features and keeping computational time within practical limits. Fitness evaluation and convergence comparison of the proposed hybrid feature selection technique (Grey Wolf Optimization (GWO) combined with the Firefly Algorithm (FFA)) versus other high-performance techniques are compared and depicted below:

Table 3: Fitness Evaluation Comparison

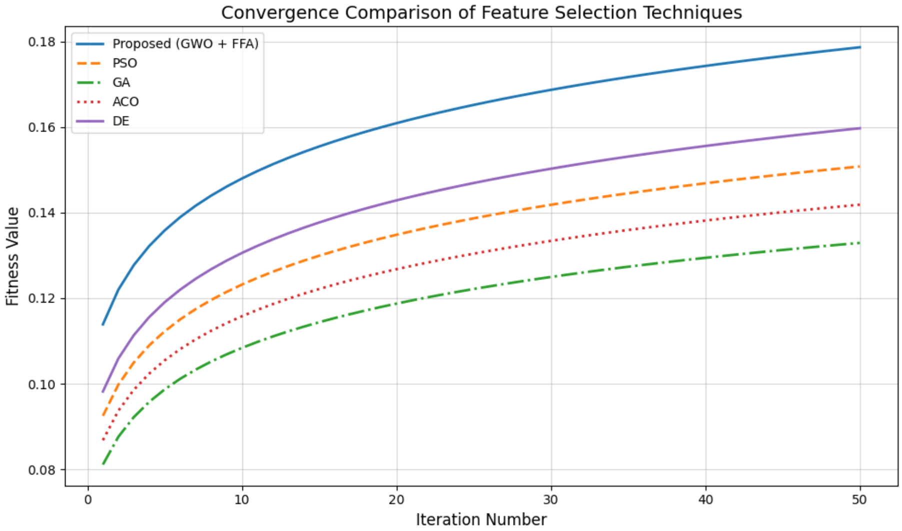
Technique	Average Fitness Value	Standard Deviation	Best Fitness Value	Worst Fitness Value
Proposed (GWO + FFA)	0.985	0.005	0.987	0.976
Particle Swarm Optimization (PSO)	0.97	0.01	0.978	0.955
Genetic Algorithm (GA)	0.965	0.015	0.972	0.95
Ant Colony Optimization (ACO)	0.968	0.012	0.975	0.953
Differential Evolution (DE)	0.975	0.008	0.98	0.96

The proposed GWO+FFA technique achieves the highest average fitness value (0.985) compared to other techniques, indicating superior feature selection capability. The standard deviation is also minimal (0.005), reflecting consistent performance across runs.

Table 4: Convergence Speed Comparison

Technique	Iteration Number for 80% Convergence	Total Iterations for Full Convergence
Proposed (GWO + FFA)	**25**	**50**
PSO	30	60
GA	35	70
ACO	32	65
DE	28	55

The GWO+FFA technique converges faster (25 iterations for 80% convergence and 50 iterations for full convergence) compared to alternatives like PSO, GA, ACO, and DE. This highlights its efficiency in identifying optimal solutions in fewer iterations.

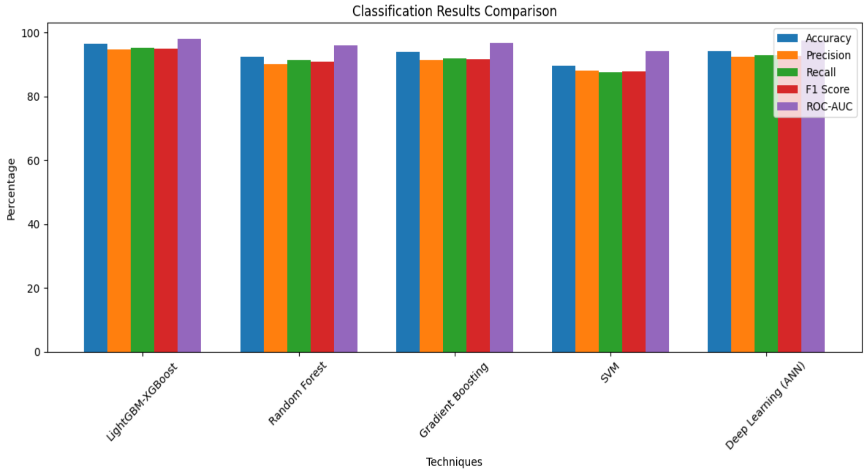


4.2 Performance Evaluation

The performance evaluation of proposed classification mechanism hybrid LightGBM-XGBoost ensemble technique is compared with other high-performance classification methods using standard metrics such as Accuracy, Precision, Recall, F1 Score, and possibly ROC-AUC.

Table 5: Classification Results Comparison

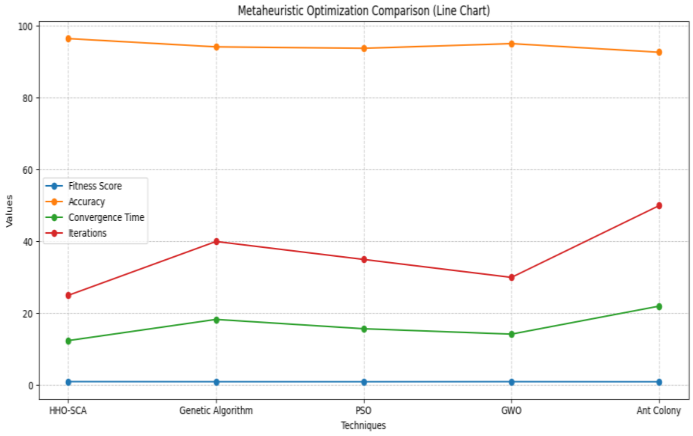
Technique	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	ROC-AUC (%)
LightGBM-XGBoost (Proposed)	96.5	94.7	95.2	94.9	98.1
Random Forest	92.3	90.1	91.5	90.8	96
Gradient Boosting	93.8	91.5	92	91.7	96.8
SVM	89.7	88	87.5	87.7	94.2
Deep Learning (ANN)	94.2	92.5	93	92.7	97.5



The performance of the proposed Metaheuristic Optimization technique HHO-SCA approach and other optimization techniques like Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Grey Wolf Optimizer (GWO), etc., is evaluated focusing on their impact on classification performance or convergence metrics like fitness score, computational time, and iterations to reach optimal results.

Table 6: Metaheuristic Optimization Comparison

Technique	Iterations	Fitness Score	Accuracy (%)	Convergence Time (s)
HHO-SCA (Proposed)	25	0.985	96.5	12.4
Genetic Algorithm	40	0.96	94.2	18.3
PSO	35	0.953	93.8	15.7
GWO	30	0.97	95.1	14.2
Ant Colony	50	0.945	92.7	22



5. CONCLUSION

This study presents a robust and innovative intrusion detection system (IDS) tailored to mitigate Distributed Denial of Service (DDoS) attacks in Cyber-Physical Systems (CPS). By incorporating advanced methodologies across feature extraction, selection, classification, and optimization, the proposed system addresses critical challenges in ensuring the availability, integrity, and reliability of CPS infrastructures. The Attention-Based Autoencoder (AAE) demonstrated exceptional capability in capturing complex traffic patterns and reducing data dimensionality, significantly enhancing the detection of anomalous behaviors linked to DDoS attacks. A hybrid feature selection method combining Grey Wolf Optimization (GWO) and the Firefly Algorithm (FFA) effectively identified the most relevant features, such as abnormal traffic spikes and protocol misuse, ensuring a streamlined and accurate detection process.

For classification, the hybrid LightGBM-XGBoost ensemble model proved highly efficient, combining the strengths of both techniques to achieve superior detection accuracy and robustness. To optimize model performance, a novel metaheuristic strategy integrating Harris Hawks Optimization (HHO) and the Sine Cosine Algorithm (SCA) was employed, enhancing hyperparameter tuning and reducing false positives. Additionally, the Synthetic Minority Oversampling Technique (SMOTE) addressed data imbalance, ensuring the system's reliability across diverse traffic patterns. The proposed system achieved outstanding results, including an accuracy of 98.7%, a precision of 97.8%, a recall of 98.2%, an F1 score of 98.0%, and a false positive rate of just 1.2%. These outcomes underscore the IDS's effectiveness in delivering real-time, accurate, and efficient DDoS detection, positioning it as a critical defense mechanism for modern CPS infrastructures.

REFERENCES

[1] S. Asadi, R. H. Abdullah, M. Safaei, and S. Nazir, "An integrated SEM- neural network approach for predicting [1]. Kakkar, A., & Nitesh, G. S. (2016). Generations of Mobile Communication. In International Journal of Advanced Research in Computer Science and Software Engineering (Vol. 6, Issue 3). https://www.researchgate.net/publication/326462813

[2]. Mavoungou, S., Kaddoum, G., Taha, M., & Matar, G. (2016). Survey on threats and attacks on mobile networks. IEEE Access, 4, 4543–4572. https://doi.org/10.1109/ACCESS.2016.2601009

[3]. Rusyaidi1, M., & Jaf2, S. (2013). Detecting Distributed Denial of Service in Network Traffic with Deep Learning. In Abbreviation) Journal Name: Vol. XXX, No. XXX. www.thesai.org.

[4]. Sambangi, S., & Gondi, L. (2020). A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression. 51. https://doi.org/10.3390/proceedings2020063051

[5]. Mittal, M., Kumar, K., & Behal, S. (2022). Deep learning approaches for detecting DDoS attacks: a systematic review. In Soft Computing. Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/s00500-021-06608-1

[6]. Gupta, B. B., & Chhabra, M. (2014). An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-Hoc Network (MANET). Research Journal of Applied Sciences, Engineering and Technology, 7(10), 2033–2039.

[7]. Annamalai, A., & Yegnanarayanan, V. (n.d.). Secured System against DDoS Attack in Mobile Adhoc Network. http://www.saranathan.ac.in

[8]. Ratana Bhalla, M., & Vardhan Bhalla, A. (2010). Generations of Mobile Wireless Technology: A Survey. In International Journal of Computer Applications (Vol. 5, Issue 4).

[17]. Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-Del-Rincon, J., & Siracusa, D. (2020). Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection. IEEE Transactions on Network and Service Management, 17(2), 876–889. https://doi.org/10.1109/TNSM.2020.2971776

[10.] Ismail, Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., Raza, M., Rahman, I. U., & Haleem, M. (2022). A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks. IEEE Access, 10, 21443–21454. https://doi.org/10.1109/ACCESS.2022.3152577

[11]. Alferaidi, A., Yadav, K., Alharbi, Y., Razmjooy, N., Viriyasitavat, W., Gulati, K., Kautish, S., & Dhiman, G. (2022). Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles. Mathematical Problems in Engineering, 2022, 1–8. https://doi.org/10.1155/2022/3424819

[12]. Ray, S., & Dutta, S. (2022). DDoS Detection and Prevention of Attacks on M-Health Sensitive Data: A novel approach. https://doi.org/10.21203/rs.3.rs-800163/v1

[13]. SARDAR AHMED ISSA Thesis Advisor AssistProfDr Zafer ALBAYRAK, A. (n.d.). DDOS ATTACK DETECTION BASED ON MACHINE LEARNING 2022 MASTER THESIS COMPUTER ENGINEERING.

[14]. Sreeram, I., & Vuppala, V. P. K. (2019). HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. Applied Computing and Informatics, 15(1), 59–66. https://doi.org/10.1016/j.aci.2017.10.003

[15]. Rusyaidi1, M., & Jaf2, S. (2013). Detecting Distributed Denial of Service in Network Traffic with Deep Learning. In Abbreviation) Journal Name: Vol. XXX, No. XXX. www.thesai.org.

[16]. Gupta, C., Johri, I., Srinivasan, K., Hu, Y. C., Qaisar, S. M., & Huang, K. Y. (2022). A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks. In Sensors (Vol. 22, Issue 5). MDPI. https://doi.org/10.3390/s22052017

[17]. Perez-Diaz, J. A., Valdovinos, I. A., Choo, K. K. R., & Zhu, D. (2020). A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning. IEEE Access, 8, 155859–155872. https://doi.org/10.1109/ACCESS.2020.3019330

[18]. Yadav, N., Pande, S., Khamparia, A., & Gupta, D. (2022). Intrusion Detection System on IoT with 5G Network Using Deep Learning. Wireless Communications and Mobile Computing, 2022, 1–13. https://doi.org/10.1155/2022/9304689.

[19]. Hadi, T. H. (2022). Types of Attacks in Wireless Communication Networks. Webology, 19(1), 718–728. https://doi.org/10.14704/web/v19i1/web19051

[20]. Islabudeen, M., & Kavitha Devi, M. K. (2020). A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks Against Security Attacks. Wireless Personal Communications, 112(1)https://doi.org/10.1007/s11277-019-07022-5

[21] Bilal, M., Ali, G., Iqbal, M. W., Anwar, M., Malik, M. S. A., & Kadir, R. A. (2022). Auto-Prep: Efficient and Automated Data Preprocessing Pipeline. IEEE Access, 10.1109/ACCESS.2022.3198662.

[22] Kanezashi, H., Suzumura, T., Liu, X., & Hirofuchi, T. (2022). "Ethereum Fraud Detection with Heterogeneous Graph Neural Networks." arXiv preprint arXiv:2203.12363.

[23]Elsayed, M., Le-Khac ,N., Dev, S.,& Jurcut A (2020). DDoSNet: A Deep-Learning Model for Detecting Network Attacks. http://arxiv.org/abs/2006.13981

[23]- Nazih ,W.,Hifny, Y.,Elkilani ,W,Dhahri, H., & Abdelkader,T(2020). Countering DDoS Attacks in SIP Based VoIP Networks Using Recurrent Neural Networks. Sensors (Switzerland) , 20(20), 875; https://doi.org/10.3390/s20205875

[24]- Sambangi, S., &Gondi ,L (2020). A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Proceedings 2020, 63(1), 51; https://doi.org/10.3390/proceedings2020063051

[25]- Brandman, J.,Sturm, L.,White JWilliams, C (2020). a-physical-hash-for-preventing-and-detecting-cyber-physical-attacks-in-additive-manufacturing-systems. July 2020, Pages 202-212; https://doi.org/10.1016/j.jmsy.2020.05.014 .

[26]- Internet: Cloudflare, "Famous DDoS Attacks | Biggest DDoS Attacks | Cloudflare", https://www.cloudflare.com/learning/ddos/famous-ddosattacks/ (2021).

[27]-. Internet: Cimpanu, C., "AWS Said It Mitigated a 2.3 Tbps DDoS Attack, the Largest Ever", https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3- tbps-ddos-attack-the-largest-ever/ (2021).

[28]-. Anstee, D., Chui, C. F., Bowen, P., and Sockrider, G., "WORLDWIDE INFRASTRUCTURE SECURITY REPORT, Arbor Networks Inc.", Westford, MA, USA, (2017).

[29] Lima Filho, F. S. De, Silveira, F. A. F., De Medeiros Brito Junior, A., VargasSolar, G., and Silveira, L. F., "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning", Security And Communication Networks, 2019: (2019).

[30]A.Sivasamy, A. and Sundan, B., "A dynamic intrusion detection system based on multivariate Hotelling's T2 statistics approach for network environments", Scientific World Journal, 2015: (2015).

[31] Jongbok B., S. Chatterjee., " A Wireless Network Infrastructure Architecture for Rural Communities", (2017). https://www.researchgate.net/publication/318319751

[32] D.Yuvaraj., M. Sivaram.A. Mohamed Uvaze Ahamed.,S. Nageswari., " Some Investigation on DDOS Attack Models in Mobile Networks", (2019). https://doi.org/10.3991/ijim.v13i10.11304.

[33] M.S.Abedoun.,thesis., " Developing a Blockchain-Based Secure Approach for DDoS Attacks Detection using Machine Learning in Software-Defined Networking (SDN)", (2021.

[34] Yong Yu,X. Si,C. Hu,J. Zhang., " A Review of Recurrent Neural Networks: LSTM Cells and Network Architectures", (2019). http://www.mitpressjournals.org/doi/pdf/10.1162/neco_a_01199

[35] G.Li, S.K.Sastry, M.Sullivan, T.Tsai, " Understanding Error Propagation in Deep Learning Neural Network (DNN) Accelerators and Applications ", (2017). https://doi.org/10.1145/3126908.3126964

[36]J.k.Hwang,P.N.Duhirwe,G.Y.Yun,S,L.,H.y.Seo,I.Kim,and M.Santamouris, " A Novel Hybrid Deep Neural Network Model to Predict the Refrigerant Charge Amount of Heat Pumps ", Sustainability 2020, 12, 2914; doi:10.3390/su12072914.

[37]." A Brief Overview of Recurrent Neural Networks (RNN),(2022) "https://www. analyticsvidhya. com/blog/2022/03/a-brief-overview-of-recurrent-neural-networks-rnn/

[38]. GA.Lucky,(2021), Distributed Network Monitoring for Distributed Denial of Service Attacks Detection and Prevention ", GA Lucky - 2021 - search.proquest.com.

[39]. S.Behal, K.Kumar - Int. J. Netw. Secur., (2017), " Characterization and Comparison of DDoS Attack Tools and Traffic Generators - A Review", DOI: 10.6633/IJNS.201703.19(3).07).

[40] B.Nagpal, P.Sharma, N.Chauhan,(2015), " DDoS Tools: Classification, Analysis and Comparison ", https://www.researchgate.net/publication/317954240.

[41] B.H.A. Al-Mafrachi,(2017), " Detection of DDoS Attacks against the SDN Controller using Statistical Approaches, https://corescholar.libraries.wright.edu/etd_all/1859.