Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.045794

ARTICLE

Advanced Optimized Anomaly Detection System for IoT Cyberattacks Using Artificial Intelligence

Ali Hamid Farea[1,*], Omar H. Alhazmi[1] and Kerem Kucuk[2]

[1]Department of Computer Science, Taibah University, Medina, 42315, Saudi Arabia

[2]Department of Software Engineering, Kocaeli University, Kocaeli, 41001, Turkey

*Corresponding Author: Ali Hamid Farea. Email: farea4356@gmail.com

Received: 07 September 2023 Accepted: 30 November 2023 Published: 27 February 2024

ABSTRACT

While emerging technologies such as the Internet of Things (IoT) have many benefits, they also pose considerable security challenges that require innovative solutions, including those based on artificial intelligence (AI), given that these techniques are increasingly being used by malicious actors to compromise IoT systems. Although an ample body of research focusing on conventional AI methods exists, there is a paucity of studies related to advanced statistical and optimization approaches aimed at enhancing security measures. To contribute to this nascent research stream, a novel AI-driven security system denoted as "AI2AI" is presented in this work. AI2AI employs AI techniques to enhance the performance and optimize security mechanisms within the IoT framework. We also introduce the Genetic Algorithm Anomaly Detection and Prevention Deep Neural Networks (GAADPSDNN) system that can be implemented to effectively identify, detect, and prevent cyberattacks targeting IoT devices. Notably, this system demonstrates adaptability to both federated and centralized learning environments, accommodating a wide array of IoT devices. Our evaluation of the GAADPSDNN system using the recently complied WUSTL-IIoT and Edge-IIoT datasets underscores its efficacy. Achieving an impressive overall accuracy of 98.18% on the Edge-IIoT dataset, the GAADPSDNN outperforms the standard deep neural network (DNN) classifier with 94.11% accuracy. Furthermore, with the proposed enhancements, the accuracy of the unoptimized random forest classifier (80.89%) is improved to 93.51%, while the overall accuracy (98.18%) surpasses the results (93.91%, 94.67%, 94.94%, and 94.96%) achieved when alternative systems based on diverse optimization techniques and the same dataset are employed. The proposed optimization techniques increase the effectiveness of the anomaly detection system by efficiently achieving high accuracy and reducing the computational load on IoT devices through the adaptive selection of active features.

KEYWORDS

Internet of Things; security; anomaly detection and prevention system; artificial intelligence; optimization techniques

1 Introduction

The Internet of Things (IoT) constitutes a networked system that links computing devices, physical and digital equipment, software, sensors, and individuals. These entities possess the capacity to autonomously exchange data over a network, eliminating the need for human-to-human (H2H) or human-to-computer (H2C) interactions [1]. The transformative potential of the IoT is evident across various sectors—including smart governance, learning, medical services, logistics, industry, and agriculture—as the IoT leads to greater efficiency and overall productivity at a lower cost [2]. Comprising components such as sensors and devices, the IoT connects these entities through Wi-Fi or alternative wireless technologies such as cellular networks and Bluetooth [3]. The data generated by these devices fuels analytics and drives decision-making processes [1,3]. While the advantages of the IoT are indisputable, there remains a pressing need for cost reduction, efficiency enhancement, and decision-making refinement [1–3].

IoT is a rapidly evolving technology poised to revolutionize diverse industries. However, several obstacles must be overcome [4], such as security, privacy, standardization, and device heterogeneity issues [5–7], before the IoT can realize its full potential. With the growing interconnectivity of IoT devices, the vulnerability to cyberattacks intensifies [2,5]. While artificial intelligence (AI)-based security offers a robust approach to addressing IoT security challenges [8,9], given that adversaries also often employ advanced AI techniques to breach AI-centric security measures, these must be employed in tandem with other strategies, including robust passwords, avoidance of compromised sites and links, and heightened awareness of security risks.

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are pivotal assets in enhancing IoT network security mechanisms. IDSs proficiently identify and alert against cyber-attacks that encompass unauthorized access, data confidentiality breaches, resource unavailability, and malevolent activities that align with the Confidentiality, Integrity, and Availability (CIA) triad [7,9]. However, traditional IDSs that rely on signatures or rule-based mechanisms scan network traffic for known attack patterns, rendering them inadequate against novel, emerging, and undisclosed threats [9]. These issues can be mitigated by AI-driven security strategies based on machine learning (ML) and deep learning (DL) techniques, giving rise to anomaly detection systems (ADSs) adept at uncovering nascent and previously undetected attacks within the IoT domain [10,11]. By training ML and DL models on extensive datasets—comprising system logs, network traffic, user behavior, and IoT device attributes—these models can discern malicious activities. Given the potency of AI-based IDSs, numerous organizations have adopted AI-driven security tools such as Microsoft Azure IoT Security, Amazon Web Services (AWS) IoT Device Defender, and Google Cloud IoT Security Command Center to detect and counteract cyberattacks on IoT devices [11].

As AI techniques possess the capacity to enhance other AI models, one such innovative technology that augments the AI-powered IDSs is presented in this work. The proposed approach—denoted as the Genetic Algorithm Anomaly Detection and Prevention Deep Neural Networks (GAADPSDNN) system—entails optimizing IDSs (grounded in other AI models) through the use of AI. The newly developed GAADPSDNN ensures the classification, identification, protection, and rectification of cyberattacks within the IoT realm. Characterized by superior performance and accuracy, this hybrid system integrates a genetic algorithm (GA) with ML and DL models to yield an optimized anomaly detection and prevention system (ADPS) that seamlessly and proficiently detects and thwarts malicious activities through fusion methodologies. Moreover, owing to its optimization strategies, the GAADPSDNN is capable of discerning attacks within heterogeneous IoT environments while alleviating the data processing burden on IoT devices.

The principal contributions of this research aimed at addressing IoT security issues are outlined below:

- Introducing GAADPSDNN security mechanisms underpinned by AI to combat IoT cyberattacks within both centralized and federated learning paradigms, tailored to device capabilities.
- Adoption of AI-driven optimization techniques enhancing GAADPSDNN security mechanisms, employing genetic mechanisms to amplify performance, alleviate IoT device workload, and identify critical features displaying high correlation.
- Implementation of diverse optimization approaches, including chi-squared (CS), random forest (RF), and genetic methodologies, to amplify AI-based ADS performance.
- Unveiling the interplay between IPSs and their dependence on ADSs, supplemented by a methodology to establish IPS prevention thresholds grounded in ADS outcomes.
- Analyzing and contrasting GAADPSDNN system outcomes for binary and multi-label scenarios in heterogeneous datasets.

The remainder of this article is structured into five sections. In Section 2, a comprehensive review of pertinent literature is presented and recent datasets are summarized, alongside ML and DL models that serve as IDS for IoT applications. In Section 3, we outline the architecture and implementation of the GAADPSDNN mechanism, along with the optimization techniques aimed at IoT security. In Section 4, the outcomes of the proposed GAADPSDNN system are described, along with key observations and research recommendations. The conclusions and suggestions for future research avenues are presented in Section 5.

2 Literature Review

Owing to the criticality and sensitivity of cyberattacks, in the absence of adequate protection, individuals, businesses, and organizations risk substantial financial and reputational losses. Consequently, an ample body of research has been dedicated to the mechanisms for IoT intrusion detection and prevention, giving rise to IDSs, including rule-based or signature-based IDS, learning-based IDS, network-based IDS, and heuristic-based IDS [12]. Some of these mechanisms have demonstrated effectiveness in identifying and categorizing attacks. However, as several of these methods have become outdated [11,12], the research focus has recently shifted toward rule-based or signature-based IDS and machine learning-based IDS. In line with this new research interest, in this study, emphasis is placed on the ADS-based AI security mechanism, thus avoiding the limitations of rule-based mechanisms, which rely on manually devised rules and instructions and cannot autonomously detect and adapt to novel attacks [12]. The IDS-based AI mechanism has demonstrated efficacy, capable of autonomously detecting, classifying, and adapting to new attacks by relying on anomalies. Although ADSs powered by AI offer many benefits, they also have several drawbacks, including high false-positive rates, data limitations and availability of real data, and the inability to respond to or stop attacks. This study was motivated by the need to mitigate these drawbacks, which is achieved by using the best optimization techniques to increase the true-positive rate, using a real dataset that simulates the real environment to ensure the accuracy of the results, and using an IPS that depends on the ADS to stop attacks.

Notably, ADS-based AI performance is contingent on the dataset used. Numerous datasets have been proposed by various authors—including NIMS, ISCX, DARPA-2009, CICDS2017, UNSW-NB15, NSL-KDD, and KDD99—many of which have not been effectively implemented in real-world IIoT and IoT ecosystems [13,14]. Moreover, these datasets lack focus and fail to capture the IIoT/IoT context [15,16], while certain outdated public datasets, such as CDX, KYOTO, MAWI, and Botnet datasets, have been omitted. Consequently, it is crucial to utilize high-quality datasets for AI-based

ADSs to accurately reflect real-world performance and environments. Such datasets must be current, reliable, and pertinent to the challenges faced in specific domains. As such, in this study, focus is placed on works that introduce IDS based on AI and employ high-quality, recent datasets. These datasets were generated to mirror IoT ecosystems and address the issues therein. Table 1 provides an overview of IDS-based AI security mechanisms, particularly those employing ML and DL for classifying cyberattacks based on up-to-date datasets that mimic IoT environments. These datasets (especially the Edge-IIoT dataset) contain attacks originating from various devices and represent contemporary attacks. As a result, they can be effectively applied within real-world IoT ecosystems.

Table 1: Recent studies employed ADS that reflects IoT ecosystems with up-to-date datasets

Ref./year↓	Dataset/features	Heterogeneous IoT Devices and Type of traffic	Number of attacks	IDS-based ML/DL	Accuracy	Learning approaches
[17] 2018	N-BaIoT/23 features	Implemented on nine different devices in IoT traffic and tested on two layers.	10 attacks	AE LOF SVM IF	They show the FPR and reduce false alarms.	Centralized
[18] 2019	Bot-IoT/46 features	Simulated in IoT traffic and tested on a virtual machine.	8 attacks	RNN SVM LSTM	0.9790 0.9998 0.9805	Centralized
[19] 2020	MQTTset/33 features	Implemented on 8 different devices in IoT traffic and tested on 2 layers.	5 attacks	NN DT RF NB MP GB	0.9932 0.9779 0.9942 0.9879 0.9468 0.9911	Centralized
[15] 2020	Federated TON-IOT/31 Features	Simulated in IoT traffic and tested on 3 layers.	9 attacks	N/A	N/A	N/A
[16] 2021	x-IIoTID/59 features	Simulated in IoT and IIoT traffic and tested on 3 layers.	18 attacks	DT NB SVM KNN LR DNN GRN	0.9945 0.4708 0.9814 0.9821 0.9661 0.9839 0.9946	Centralized
[20] 2021	WUSTL-IIoT/41 features	Implemented on 5 different devices in IoT and IIoT traffic and tested on 4 layers.	4 attacks	LR KNN SVM NB RF DT ANN	0.9990 0.9998 0.9964 0.9748 0.9999 0.9998 0.9964	Centralized
[14] **2022**	**Edge-IIoT set/61 Features**	**Implemented on more than 10 different devices in IoT and IIoT traffic and tested on 7 layers.**	**14 attacks**	**DT** **RF** **SVM** **KNN** **DNN**	**0.6711** **0.8083** **0.7761** **0.7918** **0.9467**	**Centralized and federated learning**

Various optimization techniques for ADSs using AI models have been introduced in recent studies, as listed in Table 2. These techniques have the objective of enhancing the performance of AI-based ADS and reducing the data processing burden on IoT devices. Notably, these optimization techniques have shown remarkable improvements in overall accuracy when compared to standard AI classifiers. While some techniques may increase the computational load, others effectively alleviate the burden on IoT devices. However, none of these techniques are capable of adaptively selecting active features. In contrast, the GAADPSDNN system proposed in this work can efficiently select active features and detect as well as prevent anomalies. Table 2 compares the accuracy achieved by the IDS mechanisms grounded in AI models, specifically multi-class models trained on the Edge-IIoT dataset, using various optimization approaches. The GAADPSDNN system demonstrates a significantly higher true-positive rate, resulting in a greater accuracy compared to that achieved in previous studies.

Table 2: Accuracy of the ADS mechanism on the Edge-IIoT set using optimization approaches

Proposed mechanism	Dataset	High-accuracy model with multi-classification	Goal and optimization approaches
[14] 2022 IDS-based DNN	Edge-IIoT set	94.67%	Detection without optimization
[21] 2022 2DF-IDS system		93.91%	Detection of security mechanisms using optimized techniques
[22] 2022 IDS-based inception time		94.94%	
[23] 2022 IDS-based Poly PCA		97.27%	
[24] 2023 IDS-based DeepAK-IoT		94.96%	
This study [GAADPSDNN] system		**98.18%**	**Detection and prevention mechanisms using optimized techniques**

3 Methodology

This study focuses on three interconnected focal points, each involving a workflow, intertwined with the others, culminating in the proposed GAADPSDNN system: (1) optimized approaches that intricately tie into the GAADPSDNN system (this forms the initial two letters of the system acronym, with "GA" denoting the genetic algorithm used for optimization); (2) IDS for identifying IoT cyberattacks and IPS for preempting such attacks within IoT; and (3) an aspect that overlaps with the preceding two goals and primarily relies on AI—comprising ML and DL techniques—to leverage device capabilities for data processing, ultimately shaping an effective IoT security system.

3.1 Proposed GAADPSDNN System

The workflow adopted in this study commenced with the collection or generation of datasets that would serve as inputs for the proposed GAADPSDNN system. To assess and validate this system, extensive testing was conducted using the Edge-IIoT dataset, which was chosen because it reflected real-world IoT scenarios and the inherent difficulty in achieving high-accuracy models within this context.

The system was further tested across heterogeneous IoT devices, encompassing various real-world attacks within IoT environments. This multifaceted evaluation served as a compass for identifying advanced anomaly detection systems with optimizations to achieve superior accuracy aligned with real-world performance. Notably, the ADPS grounded in AI security mechanisms is an intelligent system ideally suited for implementation within IoT ecosystems, provided that potential constraints—such as the capacity of IoT devices (in terms of CPU, memory, and power) to process AI algorithms—are accounted for. These constraints are integrated into the proposed GAADPSDNN system, where the feasibility of IoT devices to process ML or DL models, or both, is irrelevant.

The active features generated by IoT devices are selected using intelligent approaches known as genetic algorithms (GAs). GAs are adaptive, enabling the selection of important features with a high correlation while discarding unimportant features. The objective is to alleviate the processing and memory burden on IoT devices. Furthermore, to enhance the ADPS and improve the accuracy of the AI model in heterogeneous ecosystems, Fig. 1 illustrates the proposed GAADPSDNN system aimed at enhancing IoT security. The newly optimized dataset obtained through the GA optimization mechanism is divided into the training (80%) and testing (20%) subsets. This data is processed and trained using an efficient AI security classification mechanism (either ML or DL), tailored to achieve high accuracy based on device capabilities. Its pivotal aspect is the scoring model, which plays a crucial role in automatically determining the threshold, empowering the GAADPSDNN system to make decisions, such as generating alerts for applications or end users and determining whether to halt or continue processing device data. Notably, IPS predominantly relies on IDS outputs. The procedural details and pseudocode for the proposed GAADPSDNN system are shown below.

Pseudocode: Proposed GAADPSDNN system

```
Ability factors = [ CPU, Memory, Power]
Generated Datasets[ $N_{(Features)}$, $N_{(record)}$]
Genetic Algorithm [ $Select_{(10\ High\ correlation\ Features)}$ , $Drop_{(Other\ uncorrelation\ Features)}$]
        If ( $sum_{(10\ High\ correlation\ Features)}$ <0.8)
        $10_{Features}$ +1
  New Datasets → [ $N_{(n\ Features)}$]
  $If_{(ADS)}$ ($D_{MCs}$→L) {
  Trigger → $GAADS_{(RF|\ SVM)}$ , $Model_{(Local)}$ , $High_{(Accuracy,\ F\ score)}$
  Call → IPS Function
    $Elseif_{(ADS)}$ ($D_{PCs}$→M) {
    Trigger →$GAADS_{(RF|\ SVM|CNN|DNN)}$, $High_{(Accuracy,\ F\ score)}$
    Call → IPS Function
    $Elseif_{(ADS)}$ ($D_{SCs}$ → H) {
    Trigger → $GAADS_{(CNN|DNN)}$ , $Model_{(Local\ |\ Global)}$ , $High_{(Accuracy,\ F\ score)}$
    Call → IPS Function
          IPS Function ( ) {
    $If_{(IPS)}$ (CL == “Attack”&&“PC”≥ $Threshold_{(0.9)}$)
              Alert→ (Stop)
            $Else\ If_{(IPS)}$ (CL == “Attack”&&“PC”< $Threshold_{(0.9)}$)
                Action [ $Detect_{(New\ attack)}$ , $Update_{(Dataset)}$ , $Delete_{(Old\ Record)}$]
            $Else\ If_{(IPS)}$ (CL == “Normal”&&“PC”≥ $Threshold_{(0.9)}$)
```

(Continued)

Pseudocode (continued)

```
            $\textit{Alert(Continue)}$
        $\textit{Else If}_{(IPS)}$ $(CL == \text{“Normal”}\&\&\text{“PC”} < Threshold_{(0.9)})$
            $\textit{Action}[\ \textit{Detect}_{(New\ attack)},\ \textit{Update}_{(Dataset)},\ \textit{Delete}_{(Old\ Record)}]\}$
```

D refers to devices, while L, M, and H indicate Low, Moderate, and High, respectively. MCs: Microcontrollers, PCs: Personal Computers, CL: Class Label, PC: Ratio of class, SCs: Supercomputers, GAADS: Genetic Algorithm Anomaly Detection System.

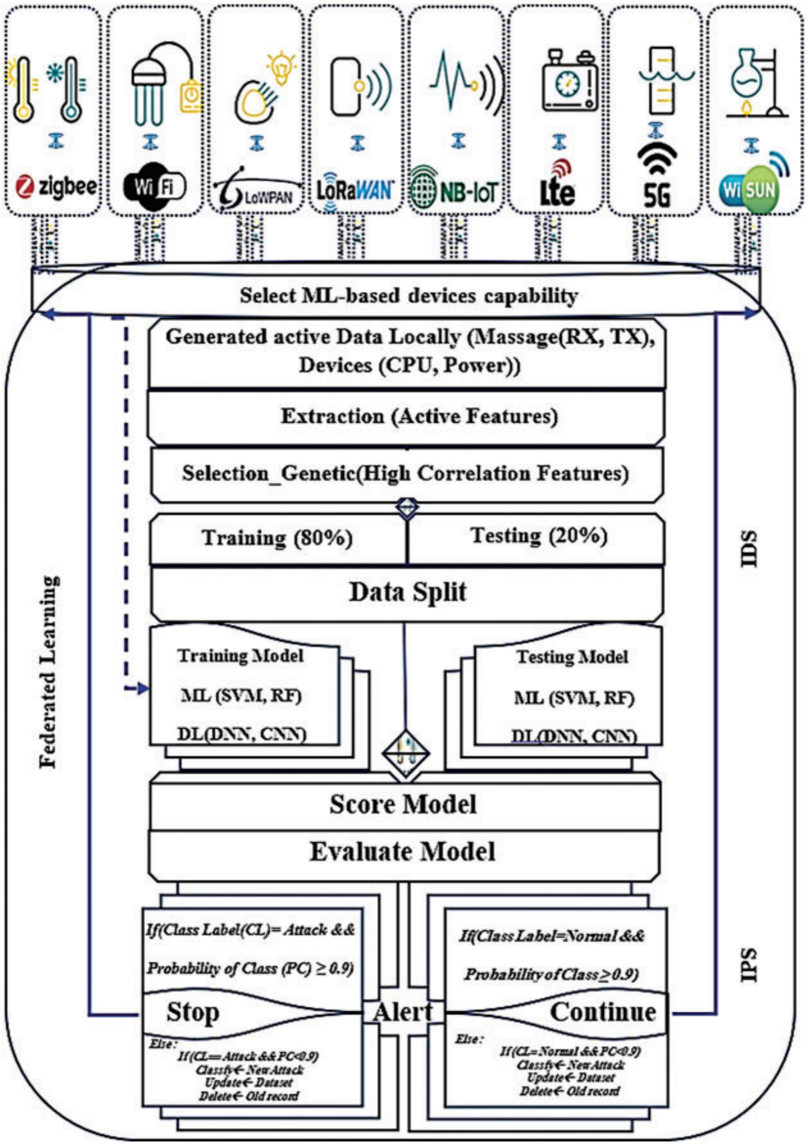


Figure 1: Proposed GAADPSDNN system for IoT security

3.2 Device Capability

Addressing the security concerns related to resource-constrained devices (i.e., those with limited CPU, memory, and power) using AI models can be challenging as such devices might struggle with processing complex models because of their inherent computational limitations. While IoT devices with substantial processing power face no such limitations and can effectively handle algorithms of significant complexity, authors of several studies have successfully implemented and deployed ML and DL algorithms on real-world, constrained IoT devices for various applications.

For instance, in extant research convolutional neural network (CNN) [25], and support vector machine (SVM) [26] have been applied to analyze videos on Raspberry Pi model 3 (ARM® v8), while human activity recognition was achieved on the ESP32 device utilizing logistic regression (LR) [27,28]. Additionally, image recognition was performed using CNN [29], SVM [30], and CNN [31] on STM32F401RE (ARM® Cortex®-M4), Raspberry Pi model 3 (ARM® v8), and Motorola 68HC11 devices. Constrained IoT devices are thus capable of running a spectrum of ML and DL algorithms, encompassing supervised, unsupervised, and reinforcement learning techniques [32]. Bringing ML and DL to the network edge enables intelligent decision-making processes on IoT devices [33,34]. It is also worth noting that numerous articles have delved into algorithm performance analysis for IoT devices [35] and the challenges related to IoT adoption, including security and privacy concerns [36].

As posited in extant studies [25–32], even devices with limited computational capacity can leverage ML and DL to address specific IoT problems. However, DL models often outperform traditional ML models in terms of accuracy, precision, and recall. Consequently, DL might be an optimal solution for identifying and classifying malicious activities in the IoT, barring limitations. Accordingly, IoT conditions, specifically device capability to process models within real-world environments, are the primary focus of the present investigation.

SVM and RF are traditional machine learning algorithms with relatively low training and deployment costs. These approaches also require less expertise to develop, train, and deploy [26,30]. Conversely, CNNs and DNNs are deep learning algorithms that have higher training and deployment, as well as expertise costs [25,29,31], but can achieve better performance on certain tasks, such as image classification and natural language processing.

This study is guided by the assumption that devices with low computational power can effectively manage IDPS-based ML in typical scenarios. In contrast, devices with substantial computational power can seamlessly handle IDPS-based DL. This approach circumvents assigning IDPS-based DL to devices lacking computational prowess. Inexpensive computational devices can handle DL, albeit not universally, due to the optimization parameters of DL algorithms that can escalate computational complexity. These parameters may impede the DL processing on devices.

The proposed GAADPSDNN system categorizes IoT devices based on their computational capabilities (assuming acceptable processing time) into three groups, denoted as low-performance, moderate-performance, and high-performance. Low-performance computational devices, such as microcontrollers or small devices, can locally process IDPS-based ML with high accuracy. Moderate-performance computational devices, including computers and tablets, can effectively manage both IDPS-based ML and DL locally with high accuracy. Finally, high-performance computational devices, such as servers, can execute IDPS-based DL with exceptional accuracy.

3.3 Data Generation and Collection

Vital parameters that are influenced by malicious activities, such as message transmitter and receiver features, should be captured as inputs for the IDS, while also incorporating device specifications such as active parameters (CPU and power). For this study, benchmark IoT datasets (generated under the IoT device conditions) were chosen to evaluate the GAADPSDNN system's efficacy in identifying malicious activities in IoT settings. As the recently compiled Edge-IIoT benchmark dataset is particularly relevant to IoT devices, it was used to compare the performance of the proposed GAADPSDNN system when applied in different contexts. Comprising 61 features, this dataset was tested across more than 10 diverse IoT devices and was assessed through 7 layers, encompassing 14 types of attacks. Researchers who conducted previous evaluations have applied DNN, SVM, KNN, DT, and RF using federated and centralized learning, whereby due to a remarkable accuracy of 94.67%, the DNN algorithm was shown to be superior to others [14].

3.4 Optimized GAADPSDNN System

Various established ML techniques, such as feature scaling and gradient descent, have been employed in extant research for optimization. In this context, CS, RF, and GA have been proven beneficial for feature selection, as these methods aid in extracting and selecting highly correlated important features, thereby reducing dataset dimensionality and thus the computational complexity of models and devices while retaining essential features. Accordingly, CS, RF, and GA techniques were harnessed in this study to optimize the proposed GAADPSDNN system.

3.4.1 Chi-Squared Approach

The chi-squared (CS) test serves as a statistical tool to assess the relationship between the dataset characteristics and the target variable. It evaluates the independence of two events by quantifying the disparity between expected and observed counts. CS operates as a nonparametric test, eschewing assumptions about data distribution. By subtracting the observed frequencies from the predicted frequencies, squaring the difference, and dividing by the expected frequency, we compute the value. CS aids in selecting filter features that elucidate the relationship between each input variable and the target variable [37]. Scrutinizing feature relationships facilitates optimal feature selection for modeling. It can be calculated using the expression below:

$$\boldsymbol{CS}^2 = \frac{\sum(\boldsymbol{AV} - \boldsymbol{EV})^2}{\boldsymbol{EV}} \tag{1}$$

where AV represents the actual value, whereas EV denotes the expected value or mean. The most significant features highlighted by the CS test in the WUSTL-IIoT dataset are displayed in Fig. 2. Fig. 3 illustrates the most important features extracted by the CS from the Edge-IIoT dataset. Notably, the CS application led to 10 essential features, discarding 31 when evaluated within the GAADPSDNN system. In dynamic environments where the expected value (EV) of the data can vary significantly, static thresholds may not be effective for anomaly/intrusion detection because a small deviation from the EV can be flagged as an anomaly during silent periods, while the same deviation may be insignificant after a heavy system load. To address this challenge, dynamic thresholds are calculated adaptively based on the current system state. In the proposed system, the threshold is calculated as the moving average of the data points over a certain period, which is equal to the average time between normal events.

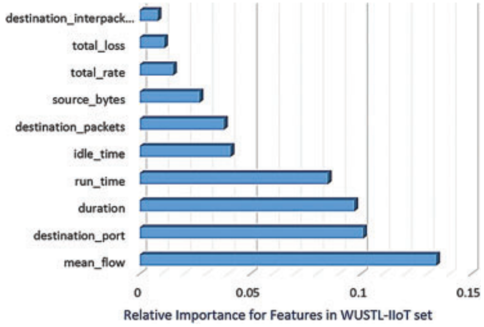


Figure 2: Selected important features extracted using the CS technique from the WUSTL-IIoT dataset

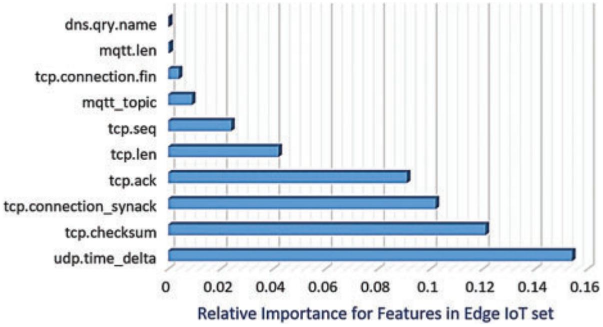


Figure 3: Important features extracted using the CS technique from the Edge-IIoT dataset

3.4.2 Random Forest Approach

Random forest (RF) is an ensemble learning (EL) method part of which multiple decision trees are constructed and their outcomes are combined to generate a final prediction. Employed as a feature selection technique in ML, RF blends filtering and wrapping benefits and can be applied even when the number of variables is large, effectively addressing the common feature selection challenges. Renowned for its predictive power, minimal overfitting issues, and high comprehensibility, RF can be used in practice to calculate feature relevance and select important features [38] using the mean decrease in Gini impurity (GI) and the mean decrease in accuracy [39], as shown below:

$$\boldsymbol{GI = 1 - \sum P^2} \tag{2}$$

where P signifies the summation of probabilities for data points assigned to a specific label (in this case either “normal” or “attack”). The primary objective of this strategy is to extract the ratio of a sample or observation belonging to a given class (normal or attack) based on a given feature (e.g., tcp.flag, tcp.connection.synack, etc.) to reduce the number of features and select the best active features from the dataset based on the GI value. The feature with the highest GI reduction among the features in the WUSTL-IIoT and Edge-IIoT datasets could potentially be the most informative. Figs. 4 and 5 depict the significant features indicated by RF within the WUSTL-IIoT and the Edge-IIoT dataset, respectively. GI is a comprehensible, calculable impurity metric, characterized by resilience against outliers, making it well-suited for RF.

3.4.3 Genetic Approach

The genetic algorithm (GA) is an optimization strategy inspired by natural selection. As GA simulates evolution to identify the optimal attribute subset, it is integrated into the proposed GAADPS-DNN system to optimize feature selection. GA applications span a wide spectrum, including the diagnosis of ongoing consciousness disorders, text classification, and high-dimensional data analysis [40,41]. Available evidence indicates that GA is adept at handling high-dimensional data and determining relevant features for specific tasks. When combined with other methods, such as SVM, rank aggregation, and genetic programming [40], GA can enhance classification performance and curtail selected feature counts [41]. The fitness function ff (Performance, Importance) shown below is used to guide the genetic algorithm's search for the optimal solution.

$$\boldsymbol{FitnessFunction} = \boldsymbol{ff}\,(Performance, Importance) \tag{3}$$

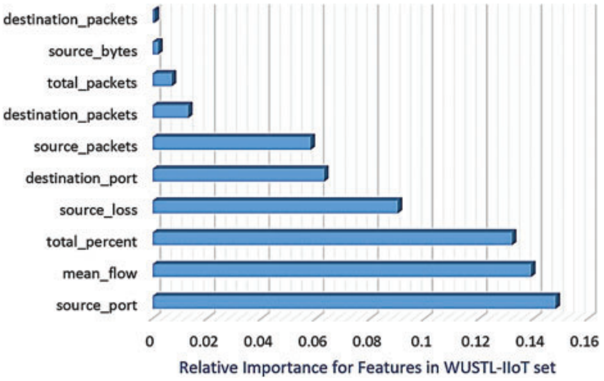


Figure 4: Important features based on the application of the RF technique to the WUSTL-IIoT dataset

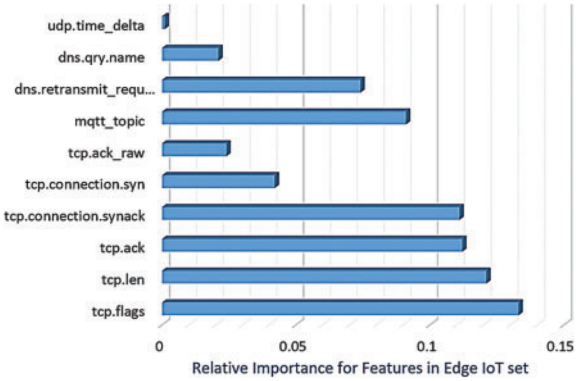


Figure 5: Important features based on the application of the RF technique to the Edge-IIoT dataset

As indicated above, ff takes two arguments—Performance (e.g., accuracy) and Relative Importance (e.g., important and unimportant features)—whereby the GA's search stops when the fitness function reaches the target (Accuracy ≥98% and Importance ≥80%) value, indicating that the current solution is the optimal solution for the proposed system. The number of selected features is adaptively changed according to incoming data to achieve the target, which leads to a decrease in the number of iterations. As indicated below, the sum of the relative importance of the correlation coefficient (CC) for significant features should be ≥0.8, while for insignificant features, it should be <0.2.

$$\text{Relative importance of the CC for fitness} = \begin{cases} \sum_{=0}^{i} \boldsymbol{CC} \geq \mathbf{0.8} & where\ \boldsymbol{i}\ for\ \boldsymbol{important}\ featuers \\ \sum_{=0}^{u} \boldsymbol{CC} < \mathbf{0.2} & where\ \boldsymbol{u}\ for\ \boldsymbol{umportant}\ featuers \end{cases} \tag{4}$$

Eq. (4) is used to control Eq. (3), which is used for the fitness function to fulfill the predefined conditions. CC's relative importance, accuracy, and precision furnish explicit fitness function measurements, enabling the proposed GAADPSDNN systems to select key features (≥0.8) with high accuracy (≥98%). Figs. 6 and 7 illustrate significant features in the WUSTL-IIoT and Edge-IIoT datasets, respectively, as determined by the GA technique.

In summary, while CS applies statistical testing for feature relevance, RF leverages ensemble learning to rank feature importance, and the GA approach employs optimization through evolutionary processes for optimal feature subsets.

As each method views feature importance differently and adheres to specific rules, all of which enhance performance and reduce IoT device load by minimizing features, their efficacy hinges on specific problem characteristics and dataset attributes. Moreover, as the sum of the relative importance of the correlation coefficients between any two points should be equal to 1 when applied to the WUSTL-IIoT dataset, CS yielded a density of 0.557 for important features and 0.443 for unimportant features. RF using Gini impurity (GI) produced densities of 0.6533 and 0.3467 for important and unimportant features, respectively. With GA employing the fitness function and our metrics, the densities for important and unimportant features were 0.886 and 0.114, respectively. This improvement underscores GA as the optimal choice, as it is capable of identifying optimal features with minimal errors (below 15%). Density visualizations for important and unimportant features in the WUSTL-IIoT dataset are depicted in Fig. 8 for CS, RF, and GA, with 41 features each. In comparison to the density of important and unimportant features in the Edge-IIoT dataset with 61 features, the density for important features using CS was 0.5477, whereas that for unimportant features was 0.4523. When the RF was applied in conjunction with GI, the density for important and unimportant features was 0.73 and 0.27, respectively. On the other hand, GA using the fitness function with our measures yielded 0.97 and 0.003, confirming that GA should be used to select the most optimal features. Fig. 9 illustrates the density of important and unimportant features in the Edge-IIoT dataset with 61 features when all three optimization mechanisms—CS, RF, and GA—were applied.

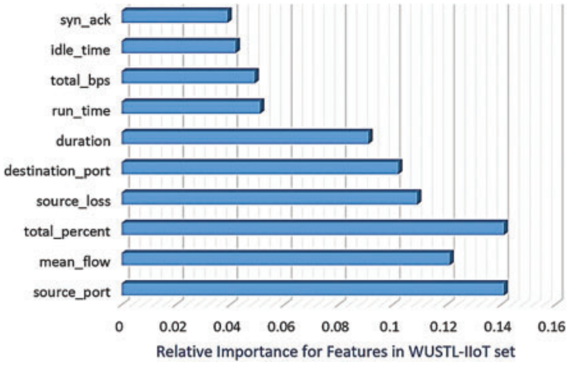


Figure 6: Important features based on the application of the GA technique on the WUSTL-IIoT dataset

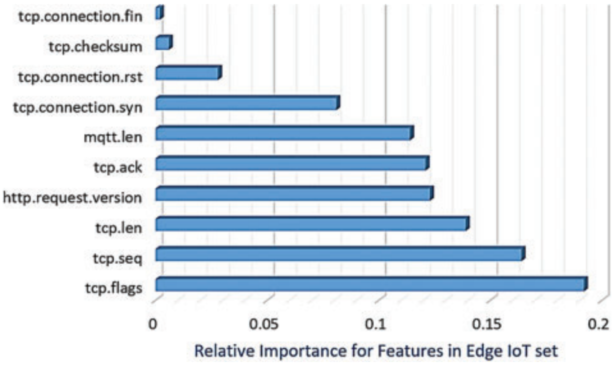


Figure 7: Important features based on the application of the GA technique on the Edge-IIoT dataset

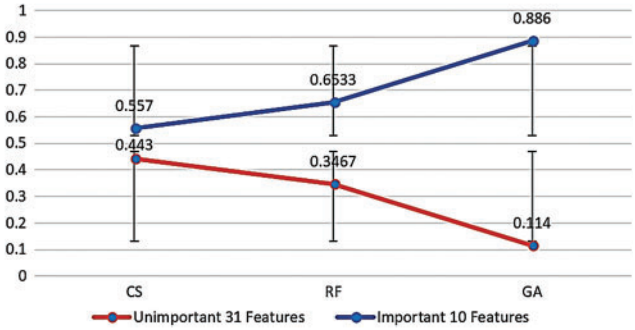


Figure 8: Density of important and unimportant features in WUSTL-IIoT dataset with 41 features

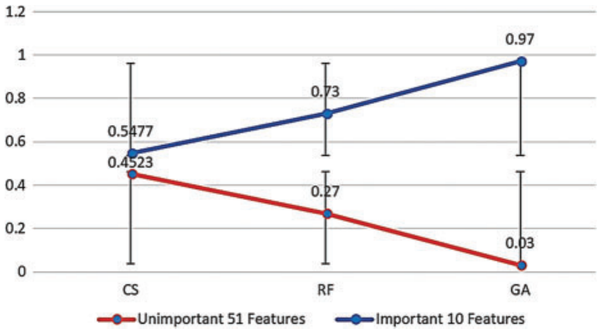


Figure 9: Density of important and unimportant features in the Edge-IIoT/IoT dataset with 61 features

3.5 *GAADSDNN Intended for Detection*

The proposed GAADPSDNN heavily relies on ML and DL to classify and detect cyberattacks and anomalies in IoT devices. Other combined AI techniques in the GAADPSDNN system are only used for optimizations aimed at enhancing performance and reducing the load on IoT devices, enabling them to function optimally. Thus, in this study, two practical ML classifiers—RF and SVM—are introduced, as both have demonstrated high processing efficiency and accuracy when executed on real IoT devices, as mentioned in Section 3.2. These classifiers are employed only on lightweight devices that lack the processing capacity needed for DL classifiers. In addition, two practical DL classifiers—CNN and DNN—are also introduced, as these deep classifier models are successfully implemented in real IoT ecosystems with high accuracy, such as video analysis and pattern recognition on Raspberry Pi devices. These classifiers are triggered only on personal computers and supercomputers that can effectively process DL classifiers. As a result, RF, SVM, CNN, and DNN are implemented in the proposed system based on the capabilities of IoT devices.

3.6 GAAPSDNN Intended for Prevention

GAAPSDNN intended for prevention primarily builds upon the GAADSDNN design used for detection. Consequently, the prevention threshold is determined by the parameter values derived from the score model results, which are scored by models such as class label (CL) and the ratio of class (PC). In our investigations, 0.9 was identified as the optimal threshold for IPS. If CL = "attack" and PC $\geq$ 0.9, the decision alerts to "stop". Otherwise, the decision involves taking action to detect new attacks, updating the dataset, and removing old records to adapt and alleviate the burden on IoT devices. Similarly, if CL = "normal" and PC $\geq$ 0.9, the decision alerts to "continue". Otherwise, the decision entails detecting new attacks, updating the dataset, and removing old records to reduce the load on IoT devices. Through this optimal threshold, the proposed GAADPSDNN mechanism permits only normal behavior to persist and halts all malicious activities.

3.7 Federated vs. Centralized Learning

Federated learning is an ML technique that trains an algorithm without transmitting data samples across several distributed edge devices or servers. Throughout the learning process, a central server manages various model steps and coordinates all participating nodes [42]. The key difference between FL and distributed learning lies in the assumptions regarding the characteristics of local datasets. While distributed learning was designed to parallelize computing capacity, FL was developed to train on heterogeneous datasets [42,43]. FL represents a privacy-preserving, decentralized strategy that is emerging as a novel approach to implementing ML. This enables mobile IoT devices to collaboratively learn a shared prediction model while retaining all training data on the device. FL optimizes the objective function and reaches consensus by training a shared model on the local datasets of all nodes. It provides a means to train AI models without exposing or accessing data, thereby enhancing data privacy and addressing security concerns. Accordingly, the GAADPSDNN system proposed in this study is adaptable to facilitate the use of FL, distributed learning, and centralized approaches for identifying anomalous IoT activities. Owing to its appealing attributes, such as adaptability with optimal features and ML and DL models based on specific operating conditions, FL and distributed learning mechanisms may offer more practical solutions for enhancing data privacy. Figs. 10 and 11 depict the GAADPSDNN system-based FL and the centralized learning model.

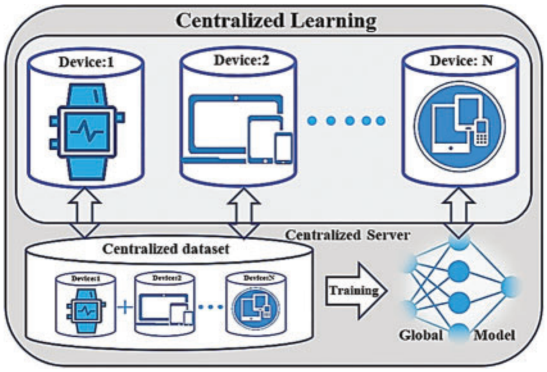


Figure 10: GAIDPSDNN system-based Centralized Learning Model

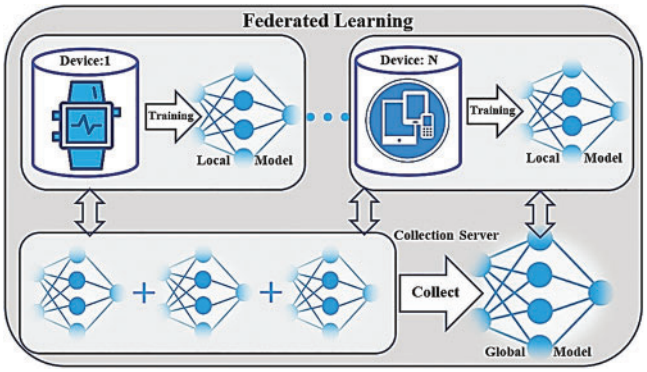


Figure 11: GAIDPSDNN system-based Federated Learning Model

4 Results and Discussion

The proposed GAADPSDNN system underwent extensive evaluation and testing in both binary and multiclass systems to compare its performance metrics on the WUSTL-IIoT and Edge-IIoT datasets. In addition, diverse optimization techniques were implemented and examined using different AI models.

4.1 GAADPSDNN Labelled with 2-Classes

The recently generated WUSTL-IIoT dataset was implemented on five distinct IoT and IIoT devices, featuring four labels or attacks categorized into “normal” or “attack” classes to allow for the evaluation of binary class performance. The WUSTL-IIoT dataset was tested using a normal classifier (NC) and various optimization techniques (including CS, RF, and GA) which were applied to two types of classifiers: ML models (RF and SVM) and DL models (CNN and DNN). As shown in Fig. 12, the binary classifier achieved a considerably higher average accuracy compared with multiclass classification. This disparity is attributed to the lower error rate within few categories. Both RF and GA yielded high optimization accuracy, demonstrating their effectiveness in enhancing the accuracy of RF, SVM, CNN, and DNN models. The binary classifier was nonetheless particularly advantageous for IDS, as it achieved high accuracy which was further augmented using optimization techniques.

A similar scenario was applied to the recently generated Edge-IIoT dataset, spanning over 10 diverse IoT and IIoT devices and tested across 7 layers with 14 attacks. The 14 labels were categorized into a single class “attack.” The Edge-IIoT set was tested with an NC and underwent various optimization techniques, such as CS, RF, and GA.

As illustrated in Fig. 13, RF and GA demonstrated high optimization accuracy in combination with the RF, SVM, CNN, and DNN models. In binary classification, the impact of optimization techniques may not be immediately evident owing to the already optimized nature of binary classification, where error rates are inherently low due to the limited number of classes. The difference between the accuracy achieved using NC and when optimization techniques are applied is marginal and nearly negligible.

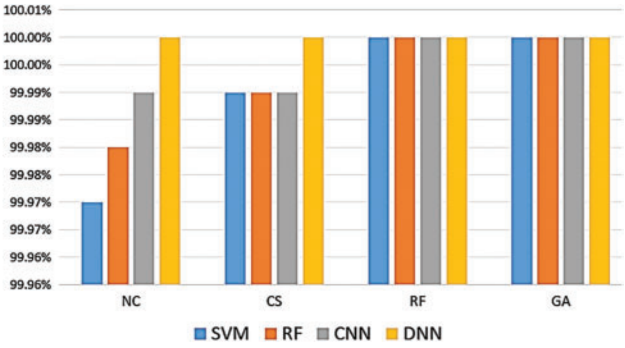


Figure 12: WUSTL-IIoT dataset with two classes

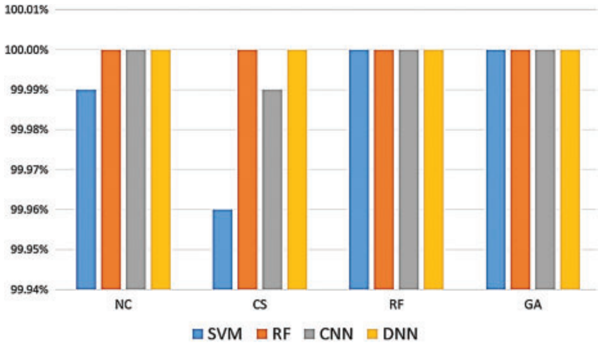


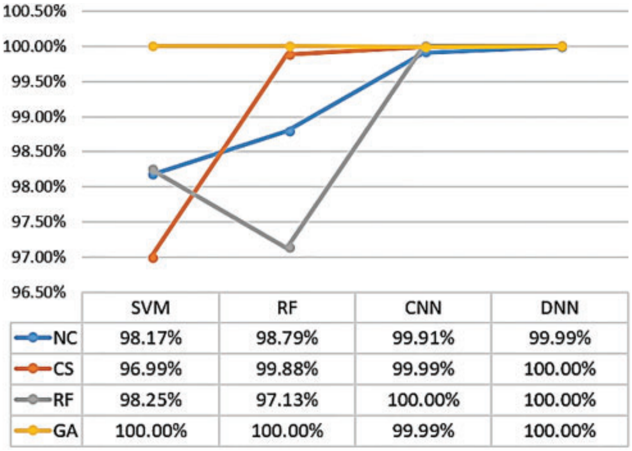
Figure 13: Edge-IIoT dataset with two labels

4.2 GAADPSDNN Labeled with the N-Class

In multiclassification, the performance matrix with optimization techniques is highly relevant and beneficial, particularly for AI classifiers, because the misclassification error rate tends to increase with the number of classes. The WUSTL-IIoT dataset, examined with a normal NC and employing various optimization techniques (including CS, RF, and GA) exhibited lower average accuracy for the multiclassifier compared with binary classification. This disparity can be attributed to the higher error rate associated with a larger number of categories. Optimization—particularly when combined with RF, SVM, CNN, and DNN models—significantly improved accuracy, as depicted in Fig. 14. Hence, these optimization techniques are valuable in achieving higher accuracy for IDS-based AI in multi-class scenarios.

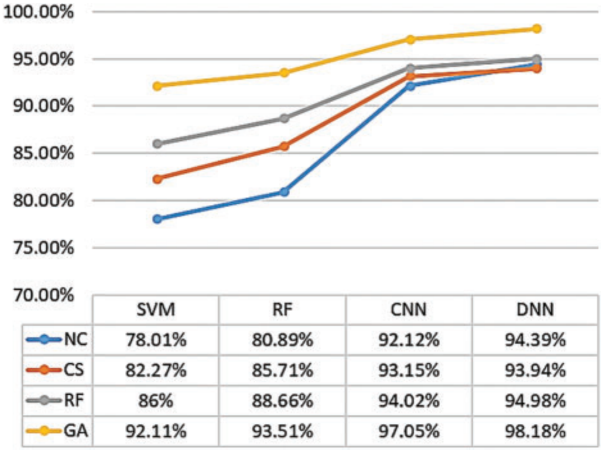
The same methodology was applied to the Edge-IIoT dataset, yielding analogous results. When these optimization techniques were tested on a multiclassifier, its accuracy was very low compared to that of binary classes, especially without optimization, due to high class-related errors and a large number of categories. The GA technique achieved high optimization accuracy when combined with RF, SVM, CNN, and DNN, as shown in Fig. 15. Therefore, the proposed optimization technique is suitable for IDS-based AI as it yields high accuracy in multiclass settings, which is further enhanced by applying the optimization techniques, especially GA followed by RF and CS, as shown in Fig. 15. However, when combined with the SVM, CNN, and DNN, both RF and GA achieve high optimization accuracy, as can be seen in Figs. 12 and 13.

The performance of binary classification with optimization techniques may not be obvious when implemented on AI workbooks because binary classification is an optimized technology and the error rate is very low because there are only two classes. The differences between the accuracy achieved with a normal classifier and when optimization techniques are applied are very slight and almost negligible. Fig. 16 shows the true-positive rate in the confusion matrix (CM) for the DNN classifier without optimization when applied to the Edge-IIoT dataset in a multiclass setting. Fig. 17 depicts the performance results such as accuracy, precision, recall, and F score of classes in the DNN without optimization. Fig. 18 shows the accuracy results after optimization. Fig. 19 also displays the CM of the optimized GAADPSDNN system.



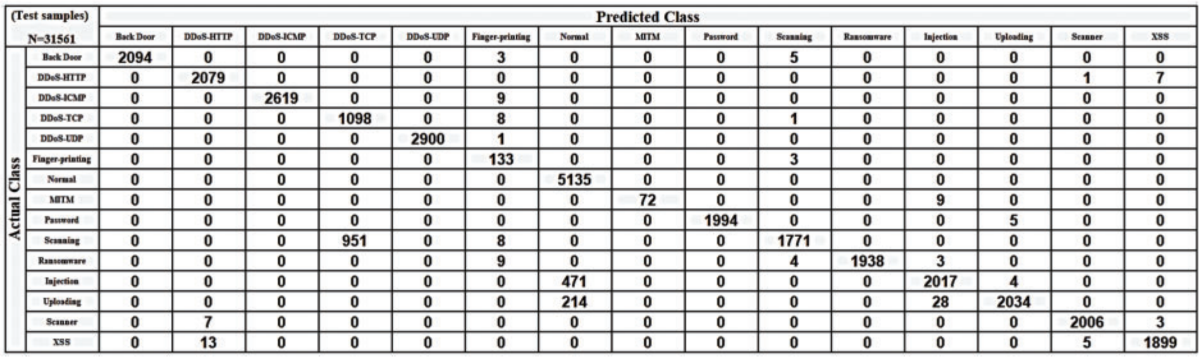
	SVM	RF	CNN	DNN
NC	98.17%	98.79%	99.91%	99.99%
CS	96.99%	99.88%	99.99%	100.00%
RF	98.25%	97.13%	100.00%	100.00%
GA	100.00%	100.00%	99.99%	100.00%

Figure 14: Accuracy results of AI classifiers with optimization approaches using the WUSTL-IIoT dataset in multiclass



	SVM	RF	CNN	DNN
NC	78.01%	80.89%	92.12%	94.39%
CS	82.27%	85.71%	93.15%	93.94%
RF	86%	88.66%	94.02%	94.98%
GA	92.11%	93.51%	97.05%	98.18%

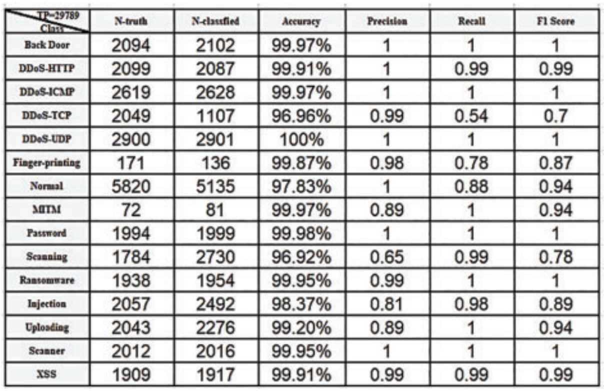
Figure 15: Accuracy results of AI classifiers with optimization approaches using the Edge-IIoT dataset in multiclass



(Test samples)		Predicted Class														
N=31561		Back Door	DDoS-HTTP	DDoS-ICMP	DDoS-TCP	DDoS-UDP	Finger-printing	Normal	MITM	Password	Scanning	Ransomware	Injection	Uploading	Scanner	XSS
Actual Class	Back Door	2094	0	0	0	0	3	0	0	0	5	0	0	0	0	0
	DDoS-HTTP	0	2079	0	0	0	0	0	0	0	0	0	0	0	1	7
	DDoS-ICMP	0	0	2619	0	0	9	0	0	0	0	0	0	0	0	0
	DDoS-TCP	0	0	0	1098	0	8	0	0	0	1	0	0	0	0	0
	DDoS-UDP	0	0	0	0	2900	1	0	0	0	0	0	0	0	0	0
	Finger-printing	0	0	0	0	0	133	0	0	0	3	0	0	0	0	0
	Normal	0	0	0	0	0	0	5135	0	0	0	0	0	0	0	0
	MITM	0	0	0	0	0	0	0	72	0	0	0	9	0	0	0
	Password	0	0	0	0	0	0	0	0	1994	0	0	0	5	0	0
	Scanning	0	0	0	951	0	8	0	0	0	1771	0	0	0	0	0
	Ransomware	0	0	0	0	0	9	0	0	0	4	1938	3	0	0	0
	Injection	0	0	0	0	0	0	471	0	0	0	0	2017	4	0	0
	Uploading	0	0	0	0	0	0	214	0	0	0	0	28	2034	0	0
	Scanner	0	7	0	0	0	0	0	0	0	0	0	0	0	2006	3
	XSS	0	13	0	0	0	0	0	0	0	0	0	0	0	5	1899

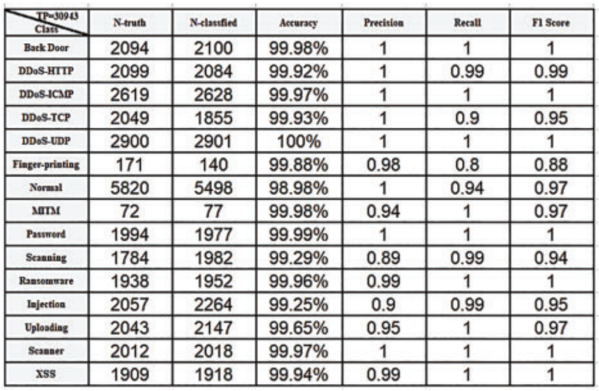
Figure 16: CM for highest accuracy AI classifiers, which DNN classifier without optimization techniques

Figs. 16–19 provide an overview of the proposed system's overall performance, as assessed via the use of a confusion matrix. The ratio associated with each class is implicit and becomes apparent through real-time testing using new data. For instance, when testing a new dataset comprising traffic records, the corresponding probabilities for each class to which a particular observation may belong are displayed. For example, if a new observation has a 0.001, 0.002, and 0.997 ratio of belonging to the "Back door attack" class, the "DDoS attack" class, and the "Normal" class, respectively, the highest ratio indicates that the new observation belongs to the "Normal" class. Consequently, the proposed system allows it to pass. Accordingly, each class is characterized by its own scored ratio, and the sum of probabilities for all classes is equal to 1. The scored label—such as "DoS attack" or "Normal"—is determined based on the highest scored ratio. To ensure that no attacks bypass the proposed system, we established an optimal ratio threshold of 0.9. Throughout the experimental phase, no scored ratio in the proposed system declined below 0.9. Consequently, the IPS is triggered based on the PC. If CL is "attack" and the PC is greater than or equal to 0.9, the decision triggers an alert to "stop". Conversely, if the PC is less than 0.9, the decision involves taking action to detect new attacks, updating the dataset, and removing outdated records to adapt and alleviate the burden on IoT devices. Likewise, if the CL is “normal” and the PC is greater than or equal to 0.9, the decision triggers an alert to “continue.”



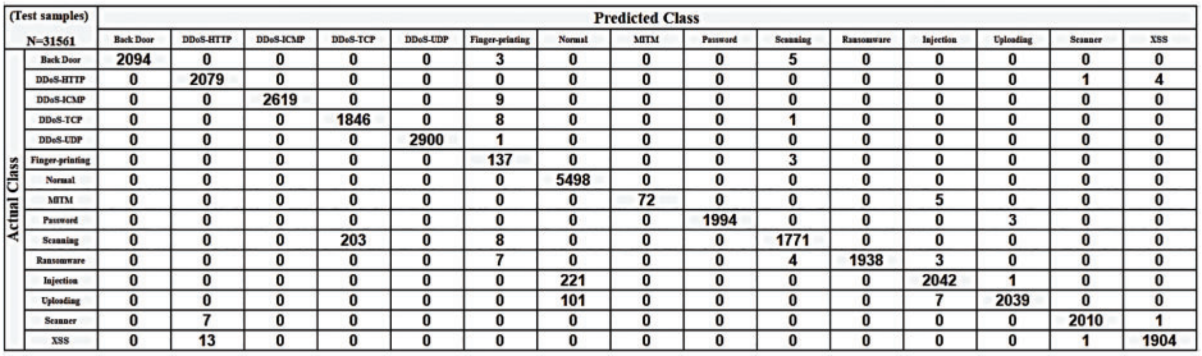
TP=29789 Class	N-truth	N-classfied	Accuracy	Precision	Recall	F1 Score
Back Door	2094	2102	99.97%	1	1	1
DDoS-HTTP	2099	2087	99.91%	1	0.99	0.99
DDoS-ICMP	2619	2628	99.97%	1	1	1
DDoS-TCP	2049	1107	96.96%	0.99	0.54	0.7
DDoS-UDP	2900	2901	100%	1	1	1
Finger-printing	171	136	99.87%	0.98	0.78	0.87
Normal	5820	5135	97.83%	1	0.88	0.94
MITM	72	81	99.97%	0.89	1	0.94
Password	1994	1999	99.98%	1	1	1
Scanning	1784	2730	96.92%	0.65	0.99	0.78
Ransomware	1938	1954	99.95%	0.99	1	1
Injection	2057	2492	98.37%	0.81	0.98	0.89
Uploading	2043	2276	99.20%	0.89	1	0.94
Scanner	2012	2016	99.95%	1	1	1
XSS	1909	1917	99.91%	0.99	0.99	0.99

Figure 17: Overall results for each class in DNN classifier without optimization using the Edge-IIoT dataset



TP=30943 Class	N-truth	N-classfied	Accuracy	Precision	Recall	F1 Score
Back Door	2094	2100	99.98%	1	1	1
DDoS-HTTP	2099	2084	99.92%	1	0.99	0.99
DDoS-ICMP	2619	2628	99.97%	1	1	1
DDoS-TCP	2049	1855	99.93%	1	0.9	0.95
DDoS-UDP	2900	2901	100%	1	1	1
Finger-printing	171	140	99.88%	0.98	0.8	0.88
Normal	5820	5498	98.98%	1	0.94	0.97
MITM	72	77	99.98%	0.94	1	0.97
Password	1994	1977	99.99%	1	1	1
Scanning	1784	1982	99.29%	0.89	0.99	0.94
Ransomware	1938	1952	99.96%	0.99	1	1
Injection	2057	2264	99.25%	0.9	0.99	0.95
Uploading	2043	2147	99.65%	0.95	1	0.97
Scanner	2012	2018	99.97%	1	1	1
XSS	1909	1918	99.94%	0.99	1	1

Figure 18: Overall results for each class in DNN classifier with optimization using the Edge-IIoT dataset



(Test samples)		Predicted Class														
N=31561		Back Door	DDoS-HTTP	DDoS-ICMP	DDoS-TCP	DDoS-UDP	Finger-printing	Normal	MITM	Password	Scanning	Ransomware	Injection	Uploading	Scanner	XSS
Actual Class	Back Door	2094	0	0	0	0	3	0	0	0	5	0	0	0	0	0
	DDoS-HTTP	0	2079	0	0	0	0	0	0	0	0	0	0	0	1	4
	DDoS-ICMP	0	0	2619	0	0	9	0	0	0	0	0	0	0	0	0
	DDoS-TCP	0	0	0	1846	0	8	0	0	0	1	0	0	0	0	0
	DDoS-UDP	0	0	0	0	2900	1	0	0	0	0	0	0	0	0	0
	Finger-printing	0	0	0	0	0	137	0	0	0	3	0	0	0	0	0
	Normal	0	0	0	0	0	0	5498	0	0	0	0	0	0	0	0
	MITM	0	0	0	0	0	0	0	72	0	0	0	5	0	0	0
	Password	0	0	0	0	0	0	0	0	1994	0	0	0	3	0	0
	Scanning	0	0	0	203	0	8	0	0	0	1771	0	0	0	0	0
	Ransomware	0	0	0	0	0	7	0	0	0	4	1938	3	0	0	0
	Injection	0	0	0	0	0	0	221	0	0	0	0	2042	1	0	0
	Uploading	0	0	0	0	0	0	101	0	0	0	0	7	2039	0	0
	Scanner	0	7	0	0	0	0	0	0	0	0	0	0	0	2010	1
	XSS	0	13	0	0	0	0	0	0	0	0	0	0	0	1	1904

Figure 19: The confusion matrix of the proposed optimized GAADPSDNN system

The proposed GAADPSDNN system leverages AI technology enhanced with additional AI techniques, resulting in high performance and accuracy across various IoT datasets and heterogeneous devices. The enhanced GAADPSDNN system’s accuracy is consistent with the values reported in other studies based on the Edge-IIoT dataset, as shown in Fig. 20.

As the heterogeneity of IoT devices makes it difficult to unify the IoT security mechanism to address security issues in all devices, this is one of the limitations of the present study.

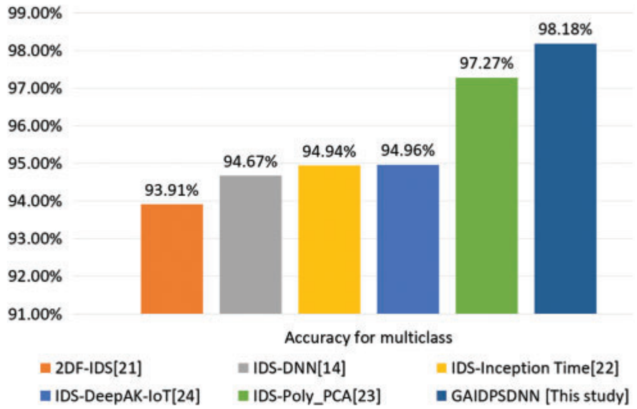


Figure 20: Comparison of the advanced GAADPSDNN system with other studies based on the Edge-IIoT dataset

5 Conclusion

As advanced attack mechanisms empowered by AI continue to emerge, the importance of AI-based security techniques becomes even more evident. Enhanced AI methods contribute to improved model accuracy and performance by alleviating the processing load. In this context, the GAADPS-DNN system was conceptualized to categorize and prevent IoT cyberattacks within heterogeneous ecosystems. It is designed to operate effectively in both FL and centralized learning settings. The proposed security system underwent thorough scrutiny and testing using contemporary optimization techniques. Its effectiveness, when coupled with optimization techniques, was demonstrated, especially when implemented on an AI classifier in multiclass scenarios. Conversely, the impact of optimization techniques on binary classification is subtle and nearly negligible. Binary classification is inherently optimized, featuring minimal error rates due to the classification of attack types into a single category called “attacks,” while regular traffic falls into the “normal” category.

The efficacy of the proposed GAADPSDNN mechanism was further evaluated by applying it to recent datasets—the WUSTL-IIoT and Edge-IIoT—related to both binary and multiclass scenarios. By implementing GA techniques and combining them with RF, SVM, CNN, and DNN classifiers, high accuracy was achieved in multiclass settings. Consequently, these optimization techniques are appropriate for IDS-based AI, as they are capable of significantly enhancing multiclass accuracy. In the context of the Edge-IIoT dataset, the GAADPSDNN mechanism demonstrated an overall accuracy of 98.18% whereas the DNN-based NC achieved 94.11%. The RF classifier’s accuracy without optimization was 80.89% and increased to 93.51% when the proposed mechanism was applied. Similarly, the CNN model achieved an overall accuracy of 97.05%, surpassing the NC’s accuracy of 92.12%. Moreover, the SVM model’s accuracy without and with optimization was 78.01% and 92.11%, respectively.

These results confirm that the GAADPSDNN system offers several benefits, including high true-positive rates, adaptive selection of active features using appropriate statistical techniques, the availability of real data, a dynamic threshold, and the ability to respond to and stop attacks while placing lower computational load on IoT devices. Overall, the GAADPSDNN system is a promising new approach to AI security with the potential to significantly impact the IoT field. It is a new AI security system that is effective, versatile, and efficient, with the potential to be widely used to protect systems from a variety of attacks.

Acknowledgement: Not applicable.

Funding Statement: The authors confirm that this study did not receive any specific funding.

Author Contributions: Study conception and design: Ali Hamid Farea; data collection: Omar H. Alhazmi; analysis and interpretation of results: Kerem Kucuk; draft manuscript preparation: Ali Hamid Farea. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The datasets used to support the findings of this study are publicly available on Kaggle https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot. Additional materials from the first author can be requested such as codes.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Liu, X. Yang, W. Wen and M. Xia, "Smarter grid in the 5G era: A framework integrating power Internet of Things with a cyber-physical system," *Frontiers in Communications and Networks*, vol. 2, pp. 1–14, 2021.

[2] P. K. Sadhu, V. P. Yanambaka and A. Abdelgawad, "Internet of Things: Security and solutions survey," *Sensors*, vol. 22, no. 19, pp. 1–51, 2022. https://doi.org/10.3390/s22197433

[3] H. Mrabet, S. Belguith, A. Alhomoud and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, pp. 3625, 2020. https://doi.org/10.3390/s20133625

[4] R. N. N. and H. V. Nath, "Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges," *Computers and Electrical Engineering*, vol. 100, pp. 107997, 2022.

[5] G. Alqarawi, B. Alkhalifah, N. H. Alharbi and S. E. Khediri, "Internet-of-Things security and vulnerabilities: Case study," *Journal of Applied Security Research*, vol. 18, no. 3, pp. 559–575, 2022.

[6] O. Ali, M. K. Ishak, M. K. L. Bhatti, I. Khan and K. Kim, "A comprehensive review of Internet of Things: Technology stack, middlewares, and fog/edge computing interface," *Sensors*, vol. 22, no. 3, pp. 995, 2022.

[7] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari *et al.,* "A survey of security and privacy issues in the Internet of Things from the layered context," *TET Technologies*, vol. 33, no. 6, pp. e3935, 2020.

[8] A. J. G. de Azambuja , C. Plesker, K. Schützer, R. Anderl, B. Schleich *et al.,* "Artificial intelligence-based cyber security in the context of Industry 4.0—A survey," *Electronics*, vol. 12, no. 8, pp. 1920, 2023.

[9] A. Attkan and V. Ranga, "Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence-based key-security," *Complex Intelligent Systems*, vol. 8, no. 4, pp. 3559–3591, 2022.

[10] S. Bi, C. Wang, J. Zhang, W. Huang, B. Wu *et al.,* "A survey on artificial intelligence aided Internet-of-Things technologies in emerging smart libraries," *Sensors*, vol. 22, no. 8, pp. 2991, 2022.

[11] R. Khilar, K. Mariyappan, M. S. Christo, J. Amutharaj, T. Anitha *et al.,* "Artificial intelligence-based security protocols to resist attacks in Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–10, 2022.

[12] A. Heidari and M. A. J. Jamali, "Internet of Things intrusion detection systems: A comprehensive review and future directions," *Cluster Computing*, vol. 26, no. 6, pp. 3753–3780, 2022.

[13] T. Hasan, J. Malik, I. Bibi, W. U. Khan, F. N. Al-Wesabi *et al.,* "Securing industrial Internet of Things against botnet attacks using hybrid deep learning approach," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2952–2963, 2023.

[14] M. A. Ferrag, O. Friha and D. Hamouda, "Edge-IIoT Set: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022.

[15] N. Moustafa, M. Keshky, E. Debiez and H. Janicke, "Federated TON_IoT windows datasets for evaluating AI-based security applications," in *Proc. of the 2020 IEEE 19th Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China, IEEE, pp. 848–855, 2020.

[16] M. Al-Hawawreh, E. Sitnikova and N. Aboutorab, "X-IIoTID: A connectivity-agnostic and device-agnostic intrusion dataset for industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3962–3977, 2021.

[17] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai *et al.,* "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.

[18] N. Koroniotis, N. Moustafa, E. Sitnikova and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[19] I. Vaccari, G. Chiola, M. Aiello and E. Cambiaso, "MQTT set: A new dataset for machine learning techniques on MQTT," *Sensors*, vol. 20, no. 22, pp. 1–17, 2020. https://doi.org/10.3390/s20226578

[20] M. Zolanvari, M. Teixeira, L. Gupta, K. Khan and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.

[21] O. Friha, M. A. Ferrag, M. Benbouzid, T. Berghout, B. Kantarci *et al.,* "2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT," *Computers & Security*, vol. 127, pp. 103097, 2023.

[22] I. Tareq, B. M. Elbagoury, S. El-Regaily and E. S. M. El-Horbaty, "Analysis of TON-IoT, UNB-NB15, and EDGE-IIoT datasets using DL in cybersecurity for IoT," *Applied Sciences*, vol. 12, no. 19, pp. 9572, 2022.

[23] P. Dini, A. Begni, S. Ciavarella, E. de Paoli, G. Fiorelli *et al.,* "Design and testing novel one-class classifier based on polynomial interpolation with application to networking security," *IEEE Access*, vol. 10, pp. 67910–67924, 2022.

[24] W. Ding, M. Abdel-Basset and R. Mohamed, "DeepAK-IoT: An effective deep learning model for cyberattack detection in IoT networks," *Information Sciences*, vol. 634, pp. 157–171, 2023.

[25] S. Y. Nikouei, Y. Chen, S. Song, R. Xu, B. Y. Choi *et al.,* "Smart surveillance as an edge network service: From Harr-cascade, SVM to a lightweight CNN," in *Proc. of the 2018 IEEE 4th Int. Conf. on Cyber Intelligence and Cyber Defense (CIC)*, Philadelphia, PA, USA, pp. 256–265, 2018.

[26] R. Xu, S. Y. Nikouei, Y. Chen, A. Polunchenko, S. Song *et al.,* "Real-time human objects tracking for smart surveillance at the edge," in *Proc. of the 2018 IEEE Int. Conf. on Communications (ICC)*, Kansas City, MO, USA, pp. 1–6, 2018.

[27] G. Chand, M. Ali, B. Barmada, V. Liesaputra and G. Ramirez-Prado, "Tracking a person's behaviour in a smart house," *Lecture Notes in Computer Science*, vol. 11434, pp. 241–252, 2019.

[28] D. Rosato, A. Masciadri, S. Comai and F. Salice, "Non-invasive monitoring system to detect sitting people," in *Proc. of the 4th EAI Int. Conf. on Smart Objects and Technologies for Social Good (SOT)*, Niagara Falls, Canada, pp. 261–264, 2018.

[29] L. T. Cook, Y. Zhu, T. J. Hall and M. F. Insana, "Bioelasticity imaging: II. Spatial resolution," *Medical Imaging 2000: Ultrasonic Imaging and Signal Processing*, vol. 3982, pp. 315–324, 2000.

[30] A. B. Flores, R. E. Guerra, E. W. Knightly, P. Ecclesine and S. Pandey, "IEEE 802.11af: A standard for TV white space spectrum sharing," *IEEE Communications Magazine*, vol. 51, no. 10, pp. 92–100, 2013.

[31] I. Lucan Orăşan, C. Seiculescu and C. D. Căleanu, "A brief review of deep neural network implementations for ARM cortex-M processor," *Electronics*, vol. 11, no. 16, pp. 2545, 2022.

[32] A. Patil, S. Iyer and R. J. Pandya, "A survey of machine learning algorithms for 6G wireless networks," arXiv preprint arXiv:2203.08429, 2022.

[33] M. Merenda, C. Porcaro and D. Iero, “Edge machine learning for AI-enabled IoT devices: A review,” *Sensors*, vol. 20, no. 9, pp. 2533, 2020.

[34] H. Wu, “Topics in deep learning and optimization algorithms for IoT applications in smart transportation,” M.S. Thesis, Dublin City University, Ireland, 2022.

[35] N. Khan, N. Sakib, I. Jerin, S. Quader and A. Chakrabarty, “Performance analysis of security algorithms for IoT devices,” in *2017 IEEE Region 10 Humanitarian Technology Conf. (R10-HTC)*, Dhaka, Bangladesh, pp. 21–23, 2017.

[36] J. Hyuk, P. Neil and Y. Yen, “Advanced algorithms and applications based on IoT for the smart devices,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1085–1087, 2018.

[37] H. Sadeghi and A. A. Raie, “HistNet: Histogram-based convolutional neural network with chi-squared deep metric learning for facial expression recognition,” *Information Sciences*, vol. 608, pp. 472–488, 2022.

[38] D. Yin, D. Chen, Y. Tang, H. Dong and X. Li, “Adaptive feature selection with shapley and hypothetical testing: Case study of EEG feature engineering,” *Information Sciences*, vol. 586, pp. 374–390, 2022.

[39] R. A. Disha and S. Waheed, “Performance analysis of machine learning models for intrusion detection system using gini impurity-based weighted random forest (GIWRF) feature selection technique,” *Cybersecurity*, vol. 5, pp. 1–22, 2022.

[40] S. Han and L. Xiao, “An improved adaptive genetic algorithm,” in *First National Conf. for Engineering Sciences (FNCES 2012)*, Baghdad, Iraq, vol. 01044, pp. 796–799, 2012.

[41] L. Ferreira, R. André, R. Backes, B. Augusto and N. Travençolo, “Optimizing a deep residual neural network with genetic algorithm for acute lymphoblastic leukemia classification,” *Journal of Digital Imaging*, vol. 35, pp. 623–637, 2022.

[42] A. M. Elbir, S. Coleri, A. K. Papazafeiropoulos, P. Kourtessis and S. Chatzinotas, “A hybrid architecture for federated and centralized learning,” *IEEE Transactions on CCN*, vol. 8, no. 3, pp. 1529–1542, 2022.

[43] B. Ghimire and D. B. Rawat, “Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things,” *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8229–8249, 2022.