IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 31 July 2024, accepted 4 August 2024, date of publication 13 August 2024, date of current version 22 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3443067

RESEARCH ARTICLE

Enhanced IoT Security for DDOS Attack Detection: Split Attention-Based ResNeXt-GRU Ensembler Approach

ABDULRAHMAN A. ALSHDADI[1], ABDULWAHAB ALI ALMAZROI[2], EESA ALSOLAMI[3], NASIR AYUB[4], (Member, IEEE), AND MILTIADIS D. LYTRAS[5], (Member, IEEE)

[1]Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia
[2]College of Computing and Information Technology at Khulais, Department of Information Technology, University of Jeddah, Jeddah 21959, Saudi Arabia
[3]Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia
[4]Department of Creative Technologies, Air University, Islamabad 44000, Pakistan
[5]Management Information Systems Department, School of Business and Economics, The American College of Greece, 153 42 Athens, Greece

Corresponding author: Nasir Ayub (nasir.ayubse@gmail.com)

This work was supported by the University of Jeddah, Jeddah, Saudi Arabia, under Grant UJ-23-SRP-13.

ABSTRACT The rising Internet of Things (IoT) device count has caused security concerns among high-tech companies and groups, which has resulted in several evaluations. IoT's pervasive, portable, and intelligent qualities make developing automated methods for spotting suspicious activity on IoT devices linked to regional infrastructure very vital. Using input factors, including network traffic attributes and output parameters, including accuracy, time complexity, and specificity, this work examines datasets, including NSL-KDD, CIC-IDS17, ToN_IoT, and UNSW-NB15. Our suggested approach uses a ResNeSt model with Split-Attention (ResNeSt), improved using the Jaya Algorithm (RSG-MJ) and augmented by a Gated Recurrent Unit (GRU). This method attained a 15% boost in efficiency considering computational complexity and an accuracy rating of 98.45%. Early-stage threat detection and computing efficiency of our system show significant advances over current techniques. The statistical analysis measures support the resilience and efficiency of our approach even more in line with the journal's goal of advancing IoT security via creative approaches. Our method is a viable solution for real-world IoT security issues as the testing results reveal its faster detection of DDoS attacks, hence improving performance.

INDEX TERMS DDOS attack, IoT, intrusion detection, deep neural networks, optimization techniques, security.

I. INTRODUCTION

The Internet of Things (IoT) has become more popular across a number of intelligent applications. Centered on gathering, analyzing, and distributing data as a consequence of continuous technical developments, Investigating developing cyber hazards in the context of IoT has taken the front stage [1]. IoT is clearly projected to be a necessary component of the next technology revolutions as its use is likely to increase drastically in the next years. Implementing strong security solutions for IoT systems is greatly difficult, given the explosion of various IoT devices and the large amounts of data they create. Maintaining data integrity in this always-changing environment depends on safeguarding IoT apps and frameworks. The network layer connections of IoT devices aggravate their susceptibility to intrusion threats by generally inadequate security measures [2].

The dispersed and resource limited character of the IoT existing systems often depends on centralized cloud-based services which introduce scalability and latency problems. With predictions indicating an estimated 76.44 billion connected devices by 2025 [3], the need for distributed, efficient, and precise detection systems becomes even more crucial. The great use of these devices increases the possibility

The associate editor coordinating the review of this manuscript and approving it for publication was Chao Tong.

for attackers to use a variety of attack routes, including interruptions in service attacks false emails and coordinated attacks, thus penetrating IoT networks. According to alarming HP studies, about seventy percent of IoT devices have security weaknesses that might be exploited in network attacks [4]. Nowadays, network attacks at the IoT's network level significantly hinder the mainstream adoption of IoT solutions.

The IoT often operates on lossy networks and has restricted resources due to its global distribution. This forces a break from traditional security paradigms in favor of customized security techniques for IoT, especially in wireless networks [5]. As they are susceptible to every part of the system, traditional defensive strategies like network security, limited access, verification, data encryption, and software security need to be revised and practical for big systems with numerous connected devices. Figure 1 [5] shows the intricate network of Service Interruption attacks directed against IoT devices.

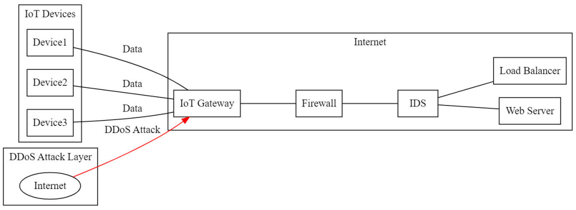


FIGURE 1. IoT layered architecture of DDoS attacks.

The present method of security threat detection in wireless networks runs within a centralized cloud, which usually fails to satisfy the many demanding needs of the IoT [6]. These needs include scalability, dispersion, limited resources, minimal latency, and more. Among linked items and groups, the IoT provides a framework allowing different communication and control activities [7]. The IoT's interface is cloud computing, which let's end users utilize a wide range of internet-based services, thereby improving speed, dependability, and accessibility [8]. In order to lower the need for human involvement, inanimate things like computers, networked devices, and equipment may autonomously share data and the external environment under this IoT framework [9]. From public safety, environmental monitoring, healthcare, industrial control, and smart homes [10], the IoT has developed into a basic infrastructure enabling many contemporary applications and services.

The growth of the IoT has coincided with the emergence of undesirable challenges that jeopardize network security, making these concerns increasingly prevalent in today's world [11]. Due to the IoT mechanism's weaknesses, a large amount of sensitive corporate data might potentially be accessed by unapproved individuals. IoT frameworks are prone to a number of privacy threats, including information monitoring, fraudulent procedures, type searching, control of malicious, and Attack Distributed Denial of Service (ADDoS) attacks [12]. IoT gadgets and services used in smart buildings might be severely impacted due to such challenges and dangers. To address those problems, educators have put forward simple solutions, such as employing algorithms based on machine learning for intrusion identification and prevention, such as SVM, naively Bayes (NB), decision forests (DT), statistical regression (LR), randomly generated forests (RF), and the use of artificial neural networks (ANN) [13].

The fog layer's nodes in the fog share responsibilities for intrusion detection inside the IoT [14]. Distributed threat detection relieves the burden of complex computations and data storage for IoT devices. Two kinds of identification of attacks are accessible for IoT devices: detection of anomalies and detection using signatures. However, each category has benefits as well as disadvantages [15]. Signature-based detection involves capturing a variety of data and processing it using predefined patterns or rules to identify threats within IoT devices. Conversely, anomalous based detection considers deviations [16] while including normal behavior patterns into the model. However, these methods could be better at detecting zero-day attacks, which are attacks that lack previous trends or established rules to be referred to.

IoT gadgets have few safety features in place to prevent threats at penetration till recent. However, as these systems demand greater processing capabilities, safeguarding them from external threats and attacks has become imperative. Ensuring security in diverse environments at the device level is challenging [17]. Although efficient, state-driven protocol approaches are expensive and protocol-specific, thorough packet analysis can cause difficulties on networks with fast speeds. In light of these drawbacks, researchers are concentrating on intrusion detectors in addition to traditional IP security protocols. Nevertheless, real-world attacks on Critical Infrastructure Systems (CPS) present significant challenges. Automatic fault recovery and device performance maintenance are the most challenging aspects of the control system [18]. The core goal of management systems is to increase the duration of regular system functioning by implementing control strategies that are able to preserve network integrity even in an environment of potential threats. Recent studies have explored the impact of metaheuristic algorithms on intrusion detection efficiency [19].

A. PROBLEM STATEMENT

One of the most significant issues in network traffic detection is being able to differentiate between legitimate activity on the network and possibly fraudulent information, which is a difficult and highly resource-intensive process [11]. Identifying the exact timing of a network breach requires analysts to sift through vast volumes of data, a process that demands significant time and effort [12], [19].

This research endeavors to develop an advanced Machine Learning (ML) model, enriched with feature reduction capabilities, to enhance the identification of network attacks within inbound network traffic. The key objective is to attain better detection efficiency and accuracy than conventional AI strategies for detection. The study's data set poses a distinct issue with respect to its large complexity and plentiful amounts of variables, which encompass both innocuous network operations and attack-related internet activity. The aim is to address this intricate problem with a novel and computationally proficient solution.

B. MOTIVATION AND CONTRIBUTION

This research is prompted by the imperative need to address the Increasing cybersecurity threats resulting from the compromise of countless vulnerable IoT devices attacking the market. The goal of the present research is to understand better why hackers are using IoT gadgets more often as destinations for ADDOS attacks [11], [14], [15], [17], [19]. The selection of devices based on IoT for conducting ADDoS has gained prominence, signifying a substantial alteration in methodologies of attack. Among the primary rationales for this modification is that such gadgets lack fundamental security attributes, which makes them extremely vulnerable to hacking. In many instances, attackers compromise one IoT device and leverage

To fill these deficiencies, our research proposes a new framework for DDoS detection that uses the ResNeSt-GRU architecture optimized with the Jaya Algorithm. To overcome the specific limitations of IoT systems, our method combines sophisticated feature extraction with time series analysis to provide a reliable outcome. Our approach is designed to enhance detection accuracy and computing efficiency, offering a viable solution for real-world applications by addressing the unique problems of IoT contexts. The following sums up our scientific advancements and their importance:

1) Data from the Real World: Our method aims to give a more thorough and justified accuracy evaluation than prior work, especially the authors' literature study, which concentrated on DDOS attack detection using Machine Learning Regression (MLR) methodologies but only took two features into account. We have meticulously gathered a data set that includes an incredible fifteen different subtypes of attacks in the local-remote risk class, seven different root-user attacks, six different probing attempts, and eleven different subtypes of attacks in the distributed service threat class.
2) Enhanced Feature Selection: We bring a new model to the field, RSG-MJ, to improve feature selection and detection accuracy.
3) Overfitting Solutions: To address the problem of overfitting, we use the Jaya Algorithm. This algorithm helps remove less important attributes, uses iterative processes to incorporate decision trees, monitors the performance of the classifier, and effectively reduces problems caused by overfitting.
4) By harnessing the computational power of a multi-layer regression (MLR) model, we can search the dataset for indicators of fraudulent activity. The area of host attack detection is much advanced by our work. Consistently sustaining both normal and attack traffic rates allows this research to pay close attention to detail, which in turn highlights the reliability of the examined features.
5) The proposed method RSG-MJ is evaluated on 4 datasets namely; NSL-KDD, CIC-IDS2017, ToN_IoT, UNSW-NB15 and achieved remarkable accuracy.
6) Using MLR and DL Regression (DLR) techniques on dynamic IoT data, our research identified safe and potentially dangerous traffic. For continuous-time traffic classification, the produced model appeared to be promising. The approach with the best classification accuracy will do well in practical settings as real-time systems generate the dataset.

Our main objectives in this work are to clarify the effects of DDoS assaults on the IoT and to provide better, more useful methods of spotting and avoiding these kinds of cyberattacks.

II. LITERATURE REVIEW

A multitude of analysts have investigated several approaches to detect and alleviate attacks with DDoS within the framework of the IoT. In [20], the author concentrated on using the Application Data Environment (ADE) in IoT networks for assessment, training, and choosing attributes, with a primary goal of identifying service interruption threats. When an information collection unit is overloaded with traffic through several sensing points, a breach of such a nature takes place. While the study aimed to organize characteristics from pre-processed data effectively, it's essential to acknowledge its limitations. The study may not encompass the full spectrum of IoT-related attacks, potentially leaving other attack vectors unaddressed. Additionally, the real-world applicability of the proposed approach needs further investigation.

In another approach, detailed in [21], the author developed an Extended Symmetric Fuzzy C-Means (ESFCM) method for IoT within a distributed threat detection system. This method presented an epidemic awareness system based on ESFCM and Fog's computing pattern. The ESFCM methodology exhibited a high detection rate, particularly due to its ability to address labeled data challenges. It's necessary to consider that the ESFCM approach's usefulness can vary based on the characteristics of a specific IoT network, and further testing on diverse IoT environments is necessary to validate its generalizability.

In 2019, as discussed in [22], the author conducted research aimed at identifying attacks on IoT-connected sensors using Machine Learning Regression (MLR) techniques. This comparative research developed a more precise way for recognizing attempts in IoT simulated settings by using a range of ML techniques to foresee deviations and attempts on IoT gadgets. Nonetheless, the study's limitations include potential challenges in handling dynamic IoT environments, as the model may need constant adaptation to emerging threats and attack patterns. Furthermore, [23] highlighted the use of data analytics as a way to identify fraudulent activities on Internet of Things devices. The study achieved higher precision than previous models by combining internet-derived input with attribute-relevant attributes from the network of smart devices. However, IoT devices with limited capabilities may struggle to implement this method due to its potential high computing resource requirements. Moreover, the method's effectiveness may be contingent on the availability of reliable external data sources.

In [24], tthe authors proposed using consensus-based trust management to identify multi-mix attacks in IoT networks. The study introduced the DCONST Model, which excelled at identifying malicious nodes and investigating attack behaviors. However, the limitations may include potential challenges in ensuring the trustworthiness of consensus-based mechanisms, as well as the need for continuous updates and adaptations as new threats emerge. Using blockchain technology, researchers in [25] presented a lightweight shared identification of anomalies approach for IoT, outperforming traditional approaches in their findings. Still, the use of blockchain technology in IoT might bring extra expense and complexity, which could restrict IoT devices with limited resources.

Author in [26] outperformed other approaches by introducing a learning-based disruption of service identification technique in IoT using an SDN Hybrid framework. However, this approach may require a more robust infrastructure, and its applicability could be constrained in IoT environments with limited resources. The author of [27] described a unique approach to threat identification in the IoT that outperformed other traditional models by combining fog computation with DLR approaches. For IoT devices with low power capacity, however, there might be restrictions like the need for significant quantities of energy and computing resources, which could be troublesome.

A connected device's aversion architecture, recognition of threats, and authority framework were described by researchers in [28], which enhanced detection performance and accuracy. However, the limitations may encompass potential difficulties in ensuring real-time threat detection and resource-intensive data processing. In [29], the author outlined a potential assault scenario in a co-located CR-IoT network, addressing threats involving harmful hidden terminals and Hidden Terminal Emulation (HTE) attacks. The limitation lies in the need for robust context-aware systems to implement the proposed detection approach effectively. A fog-based threat detection approach within the fog computing environment, introducing an ESFCM technique [30]. While the approach shows promise, it may require substantial computational resources for fog computing, and its applicability may vary depending on the specific IoT network's characteristics. Additionally, challenges related to labeled data could limit its adaptability to emerging threats.

The author of [31] presented a prescriptive maintenance (PD) algorithm that evaluated the values of IoT nodes and identified problematic nodes by utilizing the K-means algorithm and the use of a perceptron algorithm. While this model showcased improved performance and accuracy in pinpointing malicious nodes, it's worth noting that its effectiveness could be influenced by the unique characteristics of the IoT network under consideration. Moreover, it may not offer a comprehensive solution for all types of IoT-related attacks. In [32], the author presented a novel approach called the Distributed Belief Network (DBN) for Intrusion Detection Systems (IDS). This technique used layered Reduced Boltzmann Models (RBMs) to simulate the system level by level. In terms of maximum accuracy, maximum memory, and maximum recognition rates, the study showed improved performance. It is vital to recognize, nonetheless, that the DBN approach's efficacy could differ depending on the particular dataset and the type of threats it must identify. In [33], the primary focus was on the RPL protocol and a strategy for mitigating network threats. The study made use of SVELTE, a system that detects intrusion (IDS) according to specification from RPL, and an integrated IDS. Although the simulation results exhibited improved delivery rates, faster attack detection, and extended network lifetimes, the practicality of this strategy could be context-dependent, and its effectiveness might vary depending on the specific RPL attack scenarios and network configurations.

In an effort to reduce the impact of cyberattacks and restore critical systems, [34] devised a hybrid intelligent-classic control paradigm. This approach displayed improved efficiency, safety, and dependability in countering cyberattacks. Nevertheless, it's imperative to consider that the applicability of this approach could be contingent on the specific environment, and additional testing in diverse settings is warranted.

Author [35] innovatively crafted and implemented a lightweight Recurrent Neural Network (RNN)–based prediction model designed to forecast device attacks. This model outperformed traditional SVM, DT, and ANN approaches in comparing metrics of processing times, F1-rating, exactness, accuracy, and recall. Still, the specifics of the dataset and the specific attacks our model is meant to identify might affect its accuracy of predictions.

Recent advances in deep neural network (DNN) quantization and binarization have optimized network performance for resource-constrained situations. Diverse Sample Generation (DSG) discusses generative data-free quantization, which quantifies DNNs without actual data using batch normalization (BN) statistics. Increasing variety in synthetic samples improves accuracy and performance in low-bit-width circumstances, enabling effective DDoS attack detection in IoT environments [36]. Bibench benchmarks network binarization, emphasizing accuracy deterioration and efficiency issues. The benchmark highlights the impact of binarized operators on network performance and their efficiency potential on edge devices, potentially improving

DDoS detection by optimizing network resources and performance [37]. Distribution-sensitive Two-stage Estimator (DTE) and Infomax Binarization (IMB) are used in the Distribution-sensitive Information Retention Network (DIR-Net) to lower information loss in binary neural networks (BNNs). DIR-Net improves BNNs' image categorization and object identification performance by maintaining essential information during forward and backward propagation. Adopting these improvements may enhance DDoS detection systems in IoT networks by minimizing data loss while processing [38]. The keyword spotting (KWS) binary neural network BiFSMNv2 performs like a real network, saving computation and storage. BiFSMNv2 is accurate and efficient because of its dual-scale thinnable design and frequency-independent distillation. DDoS detection may benefit from fast processing and analysis of large-scale network traffic data, allowing prompt threat identification and mitigation [39]. BEBERT improves binary BERT models' accuracy and resilience using ensemble methods. Combining numerous detection models in the ensemble technique may enhance DDoS detection accuracy and resistance against complex assaults [38].

The author simulated 2D inland flood model spatio-temporal outputs using Gaussian processes. They showed that dimensionality reduction expands Gaussian process simulators, allowing accurate spatiotemporal inundation forecasts and predictive uncertainty quantification. This technique outperformed other emulation methods in consistency with flood risk maps and computational efficiency [41]. The author created a hydrodynamic simulator PINN surrogate model. Including physics based prior knowledge into the neural network design could improve model accuracy without requiring derivative calculations in the loss function. By outperforming traditional data-driven models by a margin of 25%, the PINN model proved robustness and efficiency in high resolution flood simulations [42]. Also employing Gaussian processes and convolutional autoencoders, another study projected global climate drivers. Their method taught latent space temporal dynamics and improved reduced-order models. Introducing uncertainty into the feature space led to better interpretable and confident predictions, exceeding previous approaches in efficiency and interpretability [43].

The research presented here provides useful information and methods for improving DDoS attack detection in IoT settings, particularly with regard to improving efficiency, accuracy, and resilience by means of novel quantization and binarization approaches.

III. PROPOSED SYSTEM MODEL

Deploying a robust attack detection strategy is crucial in order to effectively counteract the increasing frequency of assaults and their detrimental effects on the network resources being targeted. Several assault detection strategies have been devised, each with varying levels of efficiency, and several research have been conducted on this topic.

Our research also addresses the issue of mitigating DDOS attacks and introduces an innovative approach. Figure 2 shows a particular variant of an IDS fit for the Internet of Things. Maintaining the IoT network depends much on the server in charge of hosting the advised IDS. Starting the process falls to the sink nodes, which gather data from the end nodes of interest of the network. The sink nodes compile information and provide a thorough report to the IoT gateways. The IoT gateways act as the intermediary between the sink nodes and the server, enabling the transfer of data to the destination nodes. Important information included in this report includes IP addresses, port numbers, network protocols, data transfer speeds, and device connectivity count. Subsequently, the data undergoes normalization and multidimensional compression, often indicating potential DDoS attacks.

The processed features are then fed into a convolution feature fusion network, forming a pivotal part of the detection model. The identification of potential risks and incidents inside the IoT environment is made possible by this sophisticated network architecture. The prevention approach, which is trained to determine whether an assault is underway, is the central component of the system. This training process is a fundamental component of the proposed method, ensuring the system's ability to distinguish normal network activity from potential threats. This proposed model is systematically split into several parts, which together improve the IoT network's resilience and security.

A. DESCRIPTION OF THE DATASET AND STATISTICAL FINDINGS

Various researchers have evaluated a variety of datasets on various platforms. This investigation makes use of one of the many datasets produced by the College of New Brunswick. This development resulted from the construction of a scenario within the Canadian Institute for Cybersecurity using the NSL-KDD dataset. It was meticulously constructed by amalgamating pivotal elements with skillfully executed offensives. The repositories for data encompassed CSV files and unaltered files distinguished by the.arff and text suffixes. This file is frequently utilized when analyzing network data. To facilitate labeling, the files are separated based on the types of assault and subcategories. Figure 3 goes into depth about the data in the dataset.

IV. PRE-PROCESSING OF DATASET

In this stage, data is compiled to lay the groundwork for later ML processes and the recognition of certain trends [45]. This stage comprises several crucial elements, including the parsing and cleaning of data, the selection and extraction of features, and the separation of data into datasets for testing and training.

Data Exploring and Maintenance: It's critical to remember that the data collected in the previous phase may have been contaminated with mistakes, such as noisy data, repeated entries, and missing values. Algorithm 1 shows the essential

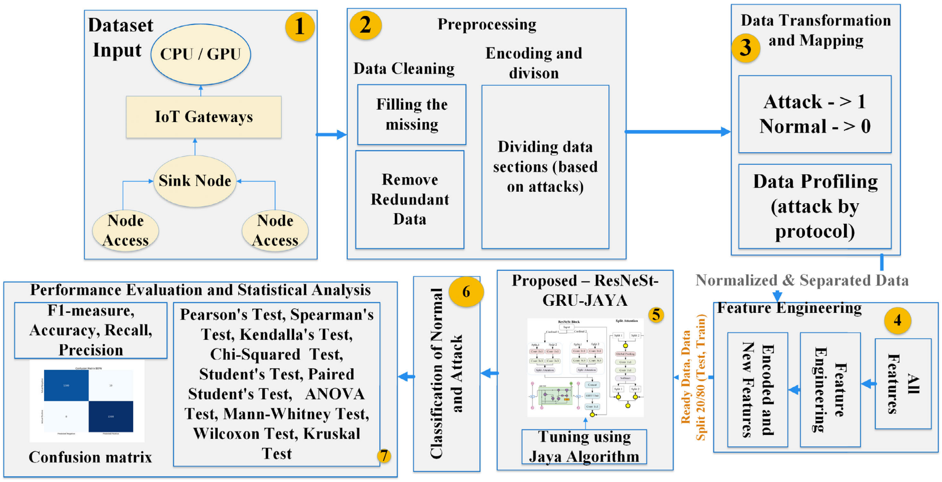
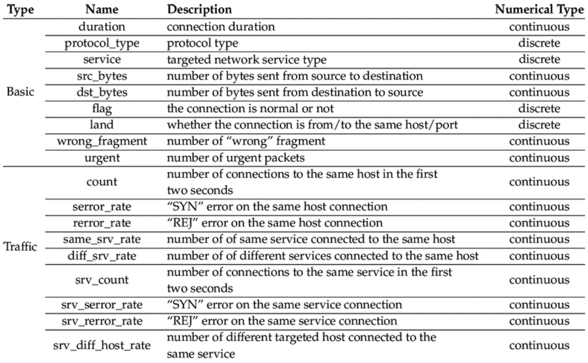

Dataset Input
1
CPU / GPU
IoT Gateways
Sink Node
Node Access
Node Access
2
Preprocessing
Data Cleaning
Encoding and divison
Filling the missing
Remove Redundant Data
Dividing data sections (based on attacks)
Data Transformation and Mapping
3
Attack - > 1
Normal - > 0
Data Profiling (attack by protocol)
Normalized & Separated Data
Feature Engineering
4
All Features
Feature Engineering
Encoded and New Features
Ready Data. Data Split 20/80 (Test, Train)
Proposed – ResNeSt-GRU-JAYA
5
Tuning using Jaya Algorithm
6
Classification of Normal and Attack
Performance Evaluation and Statistical Analysis
F1-measure, Accuracy, Recall, Precision
Confusion matrix
Pearson's Test, Spearman's Test, Kendalla's Test, Chi-Squared Test, Student's Test, Paired Student's Test, ANOVA Test, Mann-Whitney Test, Wilcoxon Test, Kruskal Test
7

FIGURE 2. Model flow for the proposed system for detecting DDoS attacks.



Type	Name	Description	Numerical Type
Basic	duration	connection duration	continuous
	protocol_type	protocol type	discrete
	service	targeted network service type	discrete
	src_bytes	number of bytes sent from source to destination	continuous
	dst_bytes	number of bytes sent from destination to source	continuous
	flag	the connection is normal or not	discrete
	land	whether the connection is from/to the same host/port	discrete
	wrong_fragment	number of "wrong" fragment	continuous
	urgent	number of urgent packets	continuous
Traffic	count	number of connections to the same host in the first two seconds	continuous
	serror_rate	"SYN" error on the same host connection	continuous
	rerror_rate	"REJ" error on the same host connection	continuous
	same_srv_rate	number of of same service connected to the same host	continuous
	diff_srv_rate	number of of different services connected to the same host	continuous
	srv_count	number of connections to the same service in the first two seconds	continuous
	srv_serror_rate	"SYN" error on the same service connection	continuous
	srv_rerror_rate	"REJ" error on the same service connection	continuous
	srv_diff_host_rate	number of different targeted host connected to the same service	continuous

FIGURE 3. Dataset features [44].

steps for having a complete understanding of the data's many facets. Each attribute is associated with a substantial quantity of data, and we modify the data to fill in any gaps. Avoiding the accumulation of duplicate data is also important. Then, using the information taken from the database, we compute the average, highest, and average deviation of the values of the attributes. This procedure guarantees that the information is ready for further ML analysis.

A. FINDING DISCREPANCIES BETWEEN THE RECOMMENDED OPTIMUM ENSEMBLE AND THE EXISTING METHODS

1) RESNEST-GRU BASED ENSEMBLER

We introduce the ResNeSt-GRU model as a pivotal component of our deep-learning approach. This model integrates the systematic acquisition and environmental comprehension skills of GRUs with the characteristics associated with the expertise in ResNeSt architectural extracting features. The flexibility of the ResNeSt-GRU model gives us the tools to create DDoS attack detection systems that operate well in the context of IoT safety, which will improve the safety of IoT gadgets and networks in the final phase. The fusion is depicted visually in Figure 4.

Algorithm 1 Data Cleaning

```
Require: Datasets containing a mixture of normal and
    abnormal data
Ensure: Purified and transformed data sets
DataCleaning: DSet
Load data from $DSet.csv$ into an array of data
for each data point $i$ in the array of data do
    Remove duplicate entries
end for
```

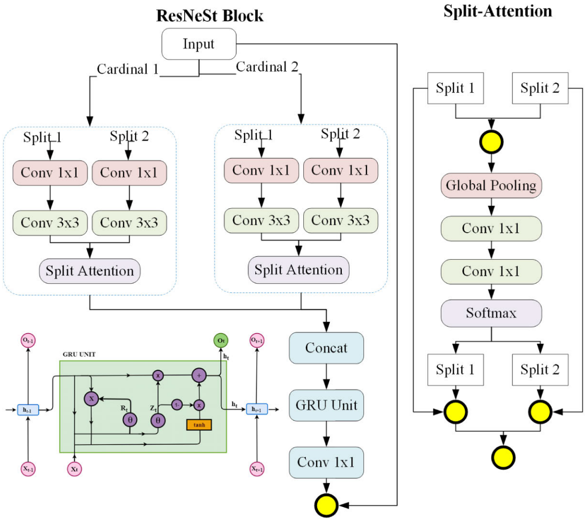


FIGURE 4. ResNeSt-GRU internal structure.

Within the domain of IoT security, the ResNeSt model serves as a vital component in our quest to enhance DDoS attack detection. For any path i inside of the ResNeSt architecture, there are actually three steps in the feature extractor procedure:

- **Convolutional Layer:** In the initial step, the input network traffic data, represented as x, undergoes a convolutional layer operation denoted as $Conv_i$. This operation is instrumental in extracting relevant features from the raw network traffic data.

- **Batch Normalization:** Following the convolutional layer, the data proceeds through batch normalization, referred to as BN_i. This step standardizes and optimizes the processed data, enhancing its suitability for subsequent DDoS attack analysis.
- **ReLU Activation:** The data undergoes processing through the Rectified Linear Unit (ReLU) activation function, represented as $ReLU_i$. By using this activation function, we make the data non-linear, which helps the model to detect ADDoS-related abnormalities and complex patterns.

The variable x represents the input network traffic data, which includes information on DDoS assaults in IoT setups. The convolution layer's output, $Conv_i$, is an important step in our algorithmic method. This layer successfully collects useful information related to DDoS assaults and prepares the data for further analysis. Following that, the data is subjected to batch normalization (BN_i), followed by the ReLU activation function ($ReLU_i$). These phases help to refine the data, making it more suitable for future processing inside route i of the ResNeSt architecture.

Our strategic approach to data processing entails splitting the information into different channels depending on the cardinality of network traffic. Each of these channels travels separately through the ResNeSt architecture, enabling them to analyze and extract distinct characteristics associated with DDoS assaults. The outputs from these different pathways are rich in unique DDoS attack-related data. These results are mixed using the Concatenation procedure. In this case, the Concatenation function effectively combines the results ($ReLU_i$) from each route, transforming their useful inputs into a complete feature map. At this step, the procedure aggregates the results from four distinct pathways.

Within the model, the concatenated feature flow reaches a critical point. A GRU layer adds a temporal component to the processing as data passes through it. The following is a dissection of the mathematical formula (Equations 1 to 4) that regulate the GRU operations [47].

$$r = \beta(Q_e \cdot [\text{Concatenation}, j_{y-1}] + v_e) \tag{1}$$

$$z = \beta(Q_x \cdot [\text{Concatenation}, j_{y-1}] + v_x) \tag{2}$$

$$\tilde{h} = \tanh(Q \cdot [\text{Concatenation}, e \cdot j_{y-1}] + v) \tag{3}$$

$$j_y = (1 - z) \cdot j_{y-1} + z \cdot \tilde{h} \tag{4}$$

These mathematical equations provide a clear understanding of the complex functioning of the GRU layer. In this instance, j_y represents the hidden state at a certain moment, y, While e and x refer to different gates controlling the information flow and the gating techniques. By use of this sequence of events, the model may effectively adapt and respond to evolving data on the DDoS attack detection in IoT environments.

2) OPTIMIZING WITH THE JAYA ALGORITHM (JA)

Hyperparameters are important components when developing deep learning models, particularly in DDoS attack detection. The framework's efficiency, generalization, and efficacy in identifying and mitigating DDoS assaults are greatly influenced by these hyperparameters. We carefully specify numerous essential hyperparameters in our work on Detecting DDoS Attacks. Table 1 provides a list of these hyperparameters.

TABLE 1. Variables optimized for the proposed RSG approach.

Hyperparameter	Optimized Value
Rate Learning	0.001
Val Decay Weight	0.0001
Epochs	50
Rate Dropout	0.3
Batch Size	64
ResNeSt Block Config	width 8, depth 64, 5 blocks
GRU Hidden Units	128

3) METRICS USED FOR PERFORMANCE EVALUATION

Upon identifying an attack, it is labeled as a true positive (TrPe), denoting the accuracy or sensitivity of the positive class. This designation is assigned when the system validates the accuracy of the detection process. In a similar vein, the system marks an instance of absence of assault as a True Negative (TrNe), indicating the Negative class's precision. On the other hand, if the system erroneously flags a non-attack as an attack, it constitutes a false positive detection (FaPe). Conversely, when the system fails to identify an actual attack, resulting in a false negative, it is termed a (FaNe). It is crucial to maintain low rates of FsPe and FaNe while prioritizing the rates of TrPe and TrNe. In addition, the F rating is calculated using a number of criteria, such as review, recall, and accuracy. Mean Absolute Error (MAE) [48], [49], [50] is another relevant statistic that quantifies the average absolute difference between yi and xi, providing a straightforward interpretation of the error margin.

a: PRECISION

Precision is a key performance indicator for assessing a predictive model's effectiveness. Regarding all events, it shows the percentage of those that fall into proper classification. Conversely, as Equation 6 shows, precision corresponds to the fraction of TrPe estimates to the total TrPe the model generates. False positive findings can have a major impact on the overall efficacy and dependability of the system, especially when it relates to DDoS attack detection and precision [50].

$$\text{Precision} = \frac{CT}{CT + IcT} \tag{5}$$

b: ACCURACY

In relation to all occurrences, indicates the proportion among occurrences that are correctly categorized. On the contrary, hand, as Equation 6 demonstrates, accuracy is related to the proportion of TrPe forecasts to the whole sum of TrPe the model produces. This ratio essentially quantifies the success rate of the predictions. Models exhibiting high accuracy are those that closely approach perfection. Especially in circumstances of an unbalanced dataset, the focus is on the capacity to reduce falsely positives and falsely negatives [50].

$$\text{Accuracy} = \frac{CT + CF}{CT + CF + IcT + IcF} \tag{6}$$

c: RECALL

Recall determines the percentage of found instances that meet a specific set of requirements, as shown in Equation 7. A measure referred to as recall measures how many beneficial results, out of all potential positive effects, were accurately anticipated. Unlike precision, which only represents the correct positive predictions, recall shows which positive predictions were not made. A measuring examination's efficiency is impacted by the number of FaPe outcomes [50].

$$\text{Recall} = \frac{CT}{CT + IcF} \tag{7}$$

d: F1-SCORE

A complete evaluation of the categorization model's effectiveness is given by the F1 score, an indicator that finds an equilibrium between both accuracy and recall. It is a useful metric for assessing model efficacy because it incorporates recall and accuracy into an individual number. The procedure that follows is used to determine the F1 score:

$$\text{F1-Score} = \text{Recall} + \text{Precision} \tag{8}$$

In this context, precision (Pre) and recall (Rec) are synonymous terms.

$$\text{Precision} = \text{Recall} \tag{9}$$

V. EXPERIMENTAL SETUP AND FINDINGS

The designated dataset was used in a simulated environment (offline) throughout the simulations. The framework described above was implemented with the optimized parameter settings mentioned, utilizing the Python language in the Spyder IDE. This study employed various frameworks, including NumPy, Matplotlib, Pandas, Keras, and other TensorFlow components.

Firstly, the computational framework is populated with data consisting of 43 attributes. The annotated data is transformed, generating binary labels (0 and 1) to enhance classification accuracy. Subsequently, the incidents are categorized based on these labels. In other words, the incidents are analyzed and classified according to different protocols, utilizing profiling data through established procedures, as detailed in the following Table 2.

After data profiling, we obtained protocol-specific attack patterns, as depicted in Figure 5. The analysis revealed that ICMP protocols primarily face attacks from the "ipsweep" method, with relatively fewer instances of attacks using the "pod" method. In difference, the TCP protocol encounters a higher frequency of attacks from the "Neptune" method. The UDP protocol, while experiencing fewer attacks overall, is predominantly targeted by the "teardrop" method.

TABLE 2. Data profiling by protocol type.

Protocol Type & Attack	TCP	UDP	ICMP
rootkit	7	3	0
Nmap	265	247	981
phf	4	0	0
smurf	0	0	2646
IMAP	11	0	0
satan	2184	1417	32
pod	0	0	201
land	18	0	0
load-module	9	0	0
Neptune	41214	0	0
passwd_guess	54	0	0
write_ftp	9	0	0
normal	53599	12434	1309
warezclient	890	0	0
warezmaster	20	0	0
port sweep	2926	0	5
spy	2	0	0
multihop	7	0	0
buffer_overflow	31	0	0
teardrop	0	892	0
upsweep	482	0	3117

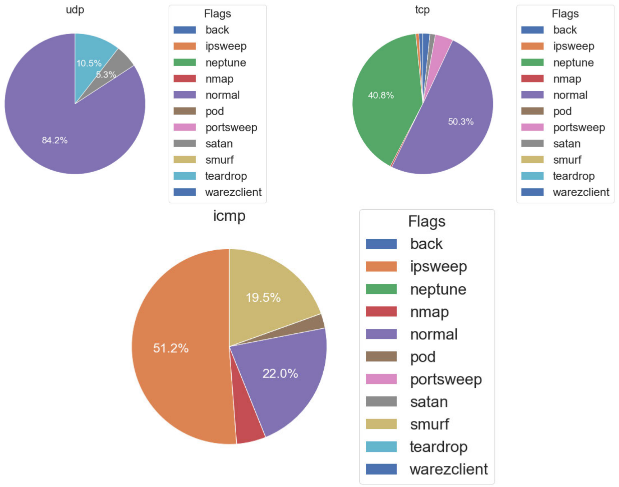


FIGURE 5. Each attack technique's strength on a certain procedure.

Our monitoring approach employs a variety of continuous network protocols, each capable of distinguishing between genuine and illicit activities. By providing historical data into our MLR model, we enabled it to effectively classify attacks like Sybil, DDoS, probe, and U2R. This method is useful for identifying and locating recurrent attack patterns, including U2R, Sybil, and probing, in long-term data on network traffic. Figure 6 displays the occurrence of every category for both allowed and illegitimate traffic.

From Figure 7, it becomes evident that a significant portion of our normal network traffic is attributed to HTTP, whereas the focus of attack traffic predominantly centers around the MCS (Mission Critical Systems). The Sybil attack is

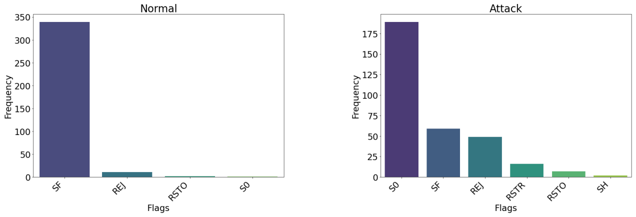


FIGURE 6. Traffic counts for both normal and attacked traffic.

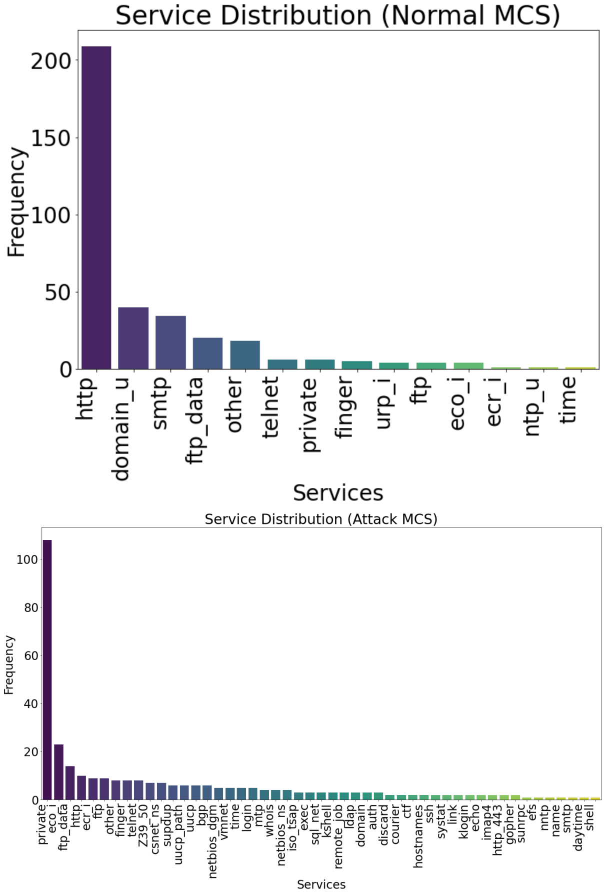


FIGURE 7. Evaluation of traffic in both regular and targeted systems.

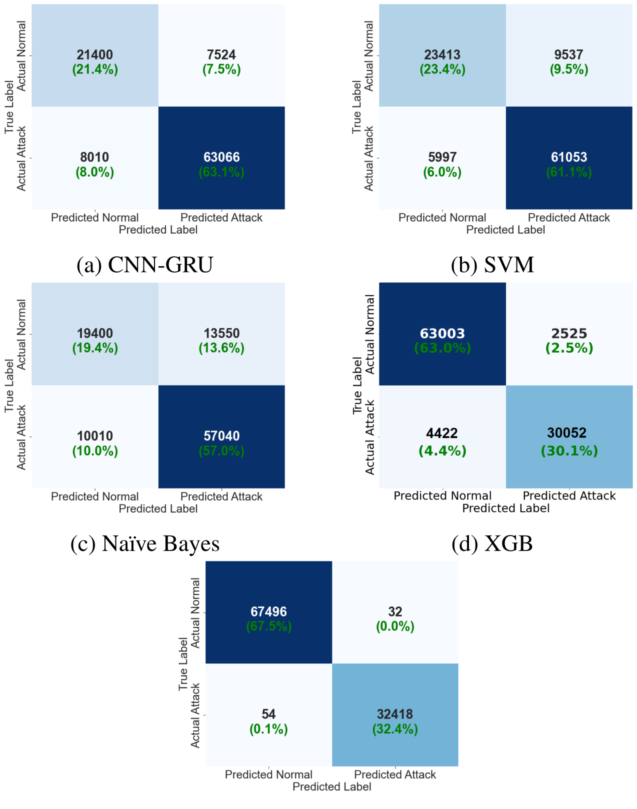
exploring various avenues to breach MCS systems, although these pathways have not yet experienced substantial traffic.

In our studies, the Jaya Algorithm was used to maximize factors like learning rates, dropout rates, and layer neuron count. With reduced computational complexity and more accuracy, this optimization approach greatly enhanced the capacity of the model to identify harmful network traffic. Comparative analysis showed that the Jaya-optimized RSG-MJ model achieved an accuracy rate of 98.45%, outperforming models that did not leverage this optimization technique. The implementation of the Jaya Algorithm contributed to a 15% increase in efficiency, highlighting its importance in enhancing the detection capabilities of our framework.

After analyzing the distribution, we utilized the DLR and MLR algorithms. The distribution of confusion for existing approaches is displayed in Figure 8. The Fn and FP rates of the existing methods are high. Compared to the RSGJ, the FP and FN rates are lower for the conventional approaches.

TABLE 3. Impact of MJ on performance metrics.

Metric	Before Optimization	After Optimization (Jaya)
Accuracy	94.32%	98.45%
Time Complexity	High	Reduced by 15%
Specificity	0.920	0.957
Precision	0.892	0.927
Recall	0.889	0.957
F1 Score	0.890	0.957



(a) CNN-GRU

(b) SVM

(c) Naïve Bayes

(d) XGB

(e) RSG-MJ (Proposed)

FIGURE 8. Matrix of confusion based on current approaches.

We analyzed the confusion matrix of the proposed method RSG-MJ as shown in Figure 9. RSG-MJ classified attack and normal values more precisely at categorizing level. Moreover, the FN and FP rates are abnormally low, indicating our method's efficiency versus previous approaches. The categorization accuracy increased after the JA provided the RSG with the required numbers. Furthermore, Figure 9 shows the ROC curve of the anticipated and present approaches. The proposed strategy has a good curve for predicting normal and attack instances.

In Figure 10, Whenever the RSG parameters are altered using the optimization method, the model's training and evaluation graph is uniform. The ensemble gets more reliable and yields consistent results with more data as its variables are improved.

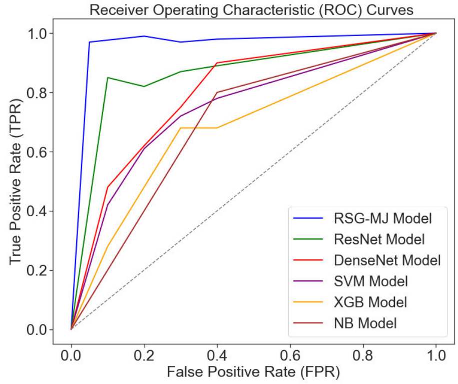
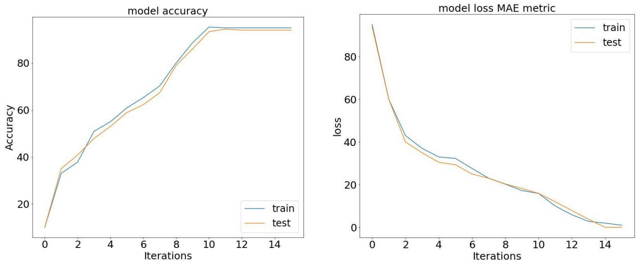


FIGURE 9. ROC assessment.



(a) Accuracy rate vs Epoch

(b) Loss rate vs Epoch

FIGURE 10. Tuned RGN.

Figure 11 computes the amount of computational work and time required for each approach. The execution time specifically refers to the testing time, which is the duration needed for the model to process and evaluate the test data after training. The RSG-MJ takes seventy seconds to run. With a lot of information, XGB has the longest execution time of 999.23 seconds.

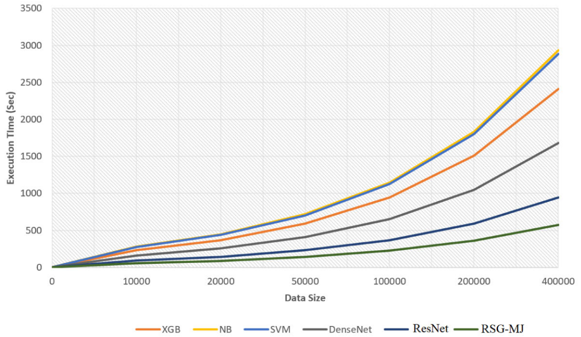


FIGURE 11. Execution complexity of proposed compared to current methods.

For the purpose of ensuring that our hypothesis is accurate, statistical analysis is performed on both the procedures that are already being used and those that have been recommended. Both Table 8 and Table 9 offer interesting analysis as a low p-value suggests that the findings show no appreciable variations. Conversely, significant discoveries are suggested by a quite large f-value higher than the critical F value from the Table. Using the F statistic, one may determine the overall influence of all of the factors. As a result of the fact that the p-value is quite low and the F-value is rather high, significant implications emerge. In situations like these, we believe that the variables that predict it and the outcome are often connected (a small F with a high p-value shows that there is no relationship between the two). The experiment's outcomes verify that our suggested method works well for promptly detecting ADDOS in the IoT.

TABLE 4. Comparing performance evaluation on NSL-KDD dataset.

Metric	RSG-MJ	ResNet	DenseNet	XGB	CNN-GRU	NB	SVM	RNN	DBN
Ref	ours	[22]	[24]	[35]	[25]	[35]	[35]	[34]	[32]
Specificity	0.957	0.896	0.883	0.902	0.850	0.861	0.878	0.871	0.888
Precision	0.927	0.818	0.807	0.828	0.771	0.780	0.814	0.801	0.820
MCC	0.957	0.841	0.830	0.852	0.795	0.804	0.827	0.815	0.833
Accuracy	0.947	0.812	0.803	0.817	0.756	0.768	0.792	0.784	0.800
G-mean	0.963	0.891	0.876	0.896	0.843	0.853	0.872	0.866	0.881
Kappa statistic	0.957	0.842	0.831	0.852	0.795	0.805	0.827	0.815	0.832
Recall	0.957	0.816	0.803	0.822	0.762	0.772	0.798	0.791	0.808
Average Precision	0.957	0.832	0.810	0.820	0.763	0.672	0.745	0.731	0.753
Log Loss	0.237	0.451	0.462	0.440	0.523	0.510	0.471	0.482	0.467
F1 Score	0.957	0.817	0.805	0.825	0.767	0.777	0.806	0.792	0.811

Table 5 evaluates many models on the CIC-IDs 2017 dataset. Our proposed method, RSG-MJ, demonstrates superior performance across all metrics, including Specificity (0.960), Precision (0.930), MCC (0.960), and Accuracy (0.950). These results indicate that RSG-MJ outperforms other models such as ResNet, DenseNet, XGB, CNN-GRU, NB, SVM, RNN, and DBN in detecting DDoS attacks, achieving the highest accuracy and lowest error rates.

TABLE 5. Benchmark comparison: performance evaluation on CIC-IDS 2017 dataset.

Metric	RSG-MJ	ResNet	DenseNet	XGB	CNN-GRU	NB	SVM	RNN	DBN
Ref	ours	[22]	[24]	[35]	[25]	[35]	[35]	[34]	[32]
Specificity	0.960	0.890	0.875	0.895	0.842	0.854	0.870	0.864	0.882
Precision	0.930	0.815	0.805	0.825	0.765	0.778	0.810	0.797	0.818
MCC	0.960	0.838	0.828	0.850	0.790	0.800	0.823	0.810	0.830
Accuracy	0.950	0.808	0.801	0.815	0.751	0.765	0.789	0.780	0.798
G-mean	0.965	0.887	0.873	0.892	0.837	0.850	0.869	0.861	0.879
Kappa statistic	0.960	0.839	0.829	0.850	0.791	0.801	0.824	0.811	0.829
Recall	0.960	0.812	0.800	0.820	0.758	0.770	0.795	0.787	0.805
Average Precision	0.960	0.828	0.808	0.818	0.758	0.670	0.740	0.727	0.750
Log Loss	0.230	0.453	0.465	0.442	0.525	0.512	0.473	0.484	0.469
F1 Score	0.960	0.814	0.803	0.822	0.762	0.775	0.802	0.788	0.809

Show the performance metrics of many models on the TON_IoT and UNSW-NB15 datasets using Table 6 and Table 7. With an accuracy of 94.68% and 94.89%, respectively, the RSG-MJ model frequently ranks second on the TON_IoT and UNSW-NB15 datasets. Indicating its remarkable capacity to detect attacks and reduce false positives precisely, it obtains the greatest precision (92.72% and 92.90%) and recall (95.69% and 95.90%), Reflecting

TABLE 6. Benchmark: performance evaluation on UNSW-NB15 dataset.

Metric	RSG-MJ	ResNet	DenseNet	XGB	CNN-GRU	NB	SVM	RNN	DBN
Ref	ours	[22]	[24]	[35]	[25]	[35]	[35]	[34]	[32]
Specificity	0.958	0.893	0.878	0.899	0.846	0.858	0.874	0.868	0.886
Precision	0.928	0.817	0.806	0.826	0.769	0.779	0.812	0.799	0.817
MCC	0.958	0.840	0.829	0.851	0.793	0.803	0.826	0.813	0.831
Accuracy	0.948	0.810	0.802	0.816	0.754	0.767	0.791	0.783	0.801
G-mean	0.964	0.889	0.874	0.894	0.841	0.852	0.870	0.864	0.880
Kappa statistic	0.958	0.841	0.830	0.851	0.794	0.804	0.826	0.814	0.830
Recall	0.958	0.814	0.801	0.821	0.760	0.771	0.797	0.789	0.806
Average Precision	0.958	0.831	0.809	0.819	0.760	0.671	0.742	0.729	0.752
Log Loss	0.233	0.450	0.461	0.438	0.521	0.508	0.469	0.481	0.465
F1 Score	0.958	0.816	0.804	0.824	0.765	0.776	0.804	0.790	0.810

TABLE 7. Benchmark: performance evaluation on TON_IoT dataset.

Metric	RSG-MJ	ResNet	DenseNet	XGB	CNN-GRU	NB	SVM	RNN	DBN
Ref	ours	[22]	[24]	[35]	[25]	[35]	[35]	[34]	[32]
Specificity	0.959	0.892	0.877	0.900	0.847	0.859	0.875	0.869	0.887
Precision	0.929	0.816	0.806	0.827	0.770	0.778	0.811	0.798	0.816
MCC	0.959	0.839	0.829	0.851	0.794	0.802	0.825	0.812	0.830
Accuracy	0.949	0.809	0.801	0.816	0.753	0.766	0.790	0.782	0.800
G-mean	0.965	0.888	0.873	0.893	0.840	0.851	0.869	0.863	0.879
Kappa statistic	0.959	0.840	0.830	0.851	0.793	0.803	0.825	0.813	0.829
Recall	0.959	0.813	0.800	0.820	0.759	0.770	0.796	0.788	0.805
Average Precision	0.959	0.830	0.809	0.819	0.759	0.670	0.741	0.728	0.751
Log Loss	0.231	0.452	0.464	0.441	0.524	0.511	0.472	0.483	0.468
F1 Score	0.959	0.815	0.804	0.823	0.764	0.775	0.803	0.789	0.808

TABLE 8. Statistical comparison of the suggested and current methods (Part 1).

Techniques	RSG-MJ		ResNet		DenseNet	
	F-stat	Pval	F-stat	Pval	F-stat	Pval
Pearson's	0.957	1.179	0.882	0	1	0
Spearman	0.952	1.14	0.866	1	1	0
Kendall a	0.759	0.971	0.795	0	1	0
Chi-Squared	3942	121	109	0	73432	0
Student a	0.235	0.021	16.356	0	2.746	0.01
Paired Student a	0.987	0.539	71.049	0	0	0

TABLE 9. Statistical comparison of the suggested and current methods (Part 2).

Techniques	SVM		NB		XGB	
	F-stat	Pval	F-stat	Pval	F-stat	Pval
Pearson's	0.859	0	0.899	0	1	0
Spearman	0.844	0	0.867	0	1	0
Kendall a	0.669	0	0.801	0	1	0
Chi-Squared	13547	0	109	0	73432	0
Student a	9.095	0	0.009	0.99	8.238	0
Paired Student a	23.88	0	0.441	0.66	0	0
ANOVA	82.71	0	0.009	0.99	67.87	0
Mann-Whitney	20718	0	41232	1	21898	0
Kreskas	82.43	0	0.001	0.98	71.22	0

its strong performance in managing unbalanced data and its excellent probability calibration, the RSG-MJ also demonstrates higher G-mean scores (96.34% and 96.50%), and the lowest Log Loss (0.237 and 0.231). This exceptional performance results from its sophisticated design integrating ResNeXt with GRU and Jaya Algorithm optimization, hence improving feature extraction and model accuracy.

VI. CONCLUSION AND FUTURE WORK

A highly efficient IDS has been built using advanced ML and DLT techniques to address the growing need for cybersecurity solutions. This study introduces a novel IDS framework called RSG-JA, which enhances feature extraction and temporal analysis capabilities. The framework is built upon the ResNeSt-GRU architecture, which has been optimized using the Jaya Algorithm. Our technique significantly enhances Internet of Things security by reducing computational complexity by 15% and increasing accuracy by 3-5% compared to earlier methods. We conducted a comprehensive evaluation of our approach using prominent datasets such as NSL-KDD, TON_IoT24, CIC-IDS17, and UNSW-NB15. The recommended approach outperformed more traditional deep and machine learning techniques in all significant performance parameters, such as accuracy, precision, false positive rate (FaPe), and true positive rate (TrPe). The findings demonstrate that our methodology effectively reduces computing expenses while accurately identifying hazards, making it a feasible choice for addressing real-world challenges pertaining to IoT security. Although these results are promising, our study does have several constraints. While comprehensive, the datasets used may only include some possible attack types or differences in IoT configurations. In addition, devices with limited computational capabilities may have difficulties while attempting to implement the ResNeSt-GRU model, mostly because of its significant depth. Future studies should improve the optimization of the model by using a larger spectrum of data and thereby overcome these constraints.

The research in this field should strive to expand the scope of threat detection to include malware assaults, ransomware, and phishing. Enhancing the model's potential to be applied to various IoT domains likehealthcare, industrial, and automotive systems, is of utmost importance. The construction of an adaptive learning system to update the model with new patterns and attacks will be of utmost importance. In addition, the use of multi-model ensemble learning techniques might potentially improve the detection of dangerous threats by reducing both false positives and false negatives. Future research should prioritize investigating the model's resilience to adversarial attacks and evaluating its performance in real-time scenarios on extensive IoT networks. The methodologies and results of the research may be extrapolated to similar cybersecurity concerns in other IoT situations. Network security may be enhanced by implementing the recommended framework on IoT gateways and edge devices. This framework enables the timely identification and prevention of DDoS attacks. The framework offers a robust solution to the challenge of safeguarding IoT systems from constantly evolving cyber threats. Its effectiveness and exceptional precision make it well-suited for environments with minimal resources.

ACKNOWLEDGMENT

This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. (UJ-23-SRP-13). The authors, therefore, thank the University of Jeddah for its technical and financial suppor

REFERENCES

[1] I. H. Sarker, "Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects," *Ann. Data Sci.*, vol. 10, no. 6, pp. 1473–1498, Dec. 2023.

[2] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, Jan. 2020.

[3] K. Maraiya and D. M. Tripathi, "IoT and its state of art applications: A survey," *Saudi J. Eng. Technol.*, vol. 7, no. 5, pp. 211–217, May 2022.

[4] M. Ahmid and O. Kazar, "A comprehensive review of the Internet of Things security," *J. Appl. Secur. Res.*, vol. 18, no. 3, pp. 289–305, Jul. 2023.

[5] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," *Sustain. Eng. Innov.*, vol. 3, no. 1, pp. 23–28, Jan. 2021.

[6] P. Musikawan, Y. Kongsorot, I. You, and C. So-In, "An enhanced deep learning neural network for the detection and identification of Android malware," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8560–8577, May 2023.

[7] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Appl. Soft Comput.*, vol. 72, pp. 79–89, Nov. 2018.

[8] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): A review," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–14, Jan. 2019.

[9] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[10] A. Rejeb, K. Rejeb, S. Simske, H. Treiblmaier, and S. Zailani, "The big picture on the Internet of Things and the smart city: A review of what we know and what we need to know," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100565.

[11] T. A. Ahanger and A. Aljumah, "Internet of Things: A comprehensive study of security issues and defense mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2019.

[12] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of Things: Evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, p. 1809, Mar. 2021.

[13] A. Churcher, R. Ullah, J. Ahmad, S. U. Rehman, F. Masood, M. Gogate, F. Alqahtani, B. Nour, and W. J. Buchanan, "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, p. 446, Jan. 2021.

[14] C. A. de Souza, C. B. Westphall, R. B. Machado, J. B. M. Sobral, and G. D. S. Vieira, "Hybrid approach to intrusion detection in fog-based IoT environments," *Comput. Netw.*, vol. 180, Oct. 2020, Art. no. 107417.

[15] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, Aug. 2020.

[16] U.-E.-H. Tayyab, F. B. Khan, M. H. Durad, A. Khan, and Y. S. Lee, "A survey of the recent trends in deep learning based malware detection," *J. Cybersecur. Privacy*, vol. 2, no. 4, pp. 800–829, Sep. 2022.

[17] H. F. Atlam and G. B. Wills, "IoT security, privacy, safety and ethics," in *Digital Twin Technologies and Smart Cities*, vol. 1. Cham, Switzerland: Springer, 2022, pp. 123–149.

[18] J.-P.-A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103201.

[19] S. S. Kareem, R. R. Mostafa, F. A. Hashim, and H. M. El-Bakry, "An effective feature selection model using hybrid metaheuristic algorithms for IoT intrusion detection," *Sensors*, vol. 22, no. 4, p. 1396, Feb. 2022.

[20] Z. A. Baig, S. Sanguanpong, S. N. Firdous, V. N. Vo, T. G. Nguyen, and C. So-In, "Averaged dependence estimators for DoS attack detection in IoT networks," *Future Gener. Comput. Syst.*, vol. 102, pp. 198–209, Jan. 2020.

[21] V. Brindha Devi, N. M. Ranjan, and H. Sharma, "IoT attack detection and mitigation with optimized deep learning techniques," *Cybern. Syst.*, vol. 55, no. 7, pp. 1702–1728, Oct. 2024.

[22] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100059.

[23] G. Rathee, S. Garg, G. Kaddoum, and B. J. Choi, "Decision-making model for securing IoT devices in smart industries," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4270–4278, Jun. 2021.

[24] Z. Ma, L. Liu, and W. Meng, "Towards multiple-mix-attack detection via consensus-based trust management in IoT networks," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101898.

[25] A. Cheema, M. Tariq, A. Hafiz, M. M. Khan, F. Ahmad, and M. Anwar, "Prevention techniques against distributed denial of service attacks in heterogeneous networks: A systematic review," *Secur. Commun. Netw.*, vol. 2022, pp. 1–15, May 2022.

[26] F. S. D. Silva, E. Silva, E. P. Neto, M. Lemos, A. J. V. Neto, and F. Esposito, "A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios," *Sensors*, vol. 20, no. 11, p. 3078, May 2020.

[27] F. Sattari, A. H. Farooqi, Z. Qadir, B. Raza, H. Nazari, and M. Almutiry, "A hybrid deep learning approach for bottleneck detection in IoT," *IEEE Access*, vol. 10, pp. 77039–77053, 2022.

[28] L. Santos, R. Gonçalves, C. Rabadão, and J. Martins, "A flow-based intrusion detection framework for Internet of Things networks," *Cluster Comput.*, vol. 26, no. 1, pp. 37–57, Feb. 2023.

[29] M. R. Babu and K. N. Veena, "A survey on attack detection methods for IoT using machine learning and deep learning," in *Proc. 3rd Int. Conf. Signal Process. Commun. (ICPSC)*, Coimbatore, India, May 2021, pp. 625–630.

[30] L. Yi, M. Yin, and M. Darbandi, "A deep and systematic review of the intrusion detection systems in the fog environment," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 1, p. 4632, Jan. 2023.

[31] L. Liu, Z. Ma, and W. Meng, "Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks," *Future Gener. Comput. Syst.*, vol. 101, pp. 865–879, Dec. 2019.

[32] A. A. Süzen, "Developing a multi-level intrusion detection system using hybrid-DBN," *J. Ambient Intell. Hum. Comput.*, vol. 12, no. 2, pp. 1913–1923, Feb. 2021.

[33] I. S. Alsukayti and A. Singh, "A lightweight scheme for mitigating RPL version number attacks in IoT networks," *IEEE Access*, vol. 10, pp. 111115–111133, 2022.

[34] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L. F. Capretz, and S. J. Abdulkadir, "Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: A systematic literature review," *Electronics*, vol. 11, no. 2, p. 198, Jan. 2022.

[35] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, and S. Gordon, "Cyberattacks detection in IoT-based smart city applications using machine learning techniques," *Int. J. Environ. Res. Public Health*, vol. 17, no. 24, p. 9347, Dec. 2020.

[36] H. Qin, Y. Ding, X. Zhang, J. Wang, X. Liu, and J. Lu, "Diverse sample generation: Pushing the limit of generative data-free quantization," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 10, pp. 11689–11706, Oct. 2023.

[37] H. Qin, M. Zhang, Y. Ding, A. Li, Z. Cai, Z. Liu, and X. Liu, "BiBench: Benchmarking and analyzing network binarization," in *Proc. Int. Conf. Mach. Learn.*, Jul. 2023, pp. 28351–28388.

[38] H. Qin, X. Zhang, R. Gong, Y. Ding, Y. Xu, and X. Liu, "Distribution-sensitive information retention for accurate binary neural network," *Int. J. Comput. Vis.*, vol. 131, no. 1, pp. 26–47, Jan. 2023.

[39] H. Qin, X. Ma, Y. Ding, X. Li, Y. Zhang, Z. Ma, J. Wang, J. Luo, and X. Liu, "BiFSMNv2: Pushing binary neural networks for keyword spotting to real-network performance," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 8, pp. 10674–10686, Aug. 2024.

[40] J. Tian, C. Fang, H. Wang, and Z. Wang, "BEBERT: Efficient and robust binary ensemble BERT," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Jun. 2023, pp. 1–5.

[41] J. Donnelly, S. Abolfathi, J. Pearson, O. Chatrabgoun, and A. Daneshkhah, "Gaussian process emulation of spatio-temporal outputs of a 2D inland flood model," *Water Res.*, vol. 225, Oct. 2022, Art. no. 119100.

[42] J. Donnelly, A. Daneshkhah, and S. Abolfathi, "Physics-informed neural networks as surrogate models of hydrodynamic simulators," *Sci. Total Environ.*, vol. 912, Feb. 2024, Art. no. 168814.

[43] J. Donnelly, A. Daneshkhah, and S. Abolfathi, "Forecasting global climate drivers using Gaussian processes and convolutional autoencoders," *Eng. Appl. Artif. Intell.*, vol. 128, Feb. 2024, Art. no. 107536.

[44] University of New Brunswick. *NSLKDD DataSet*. Accessed: Mar. 22, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html

[45] R. Zebari, A. Abdulazeez, D. Zeebaree, D. Zebari, and J. Saeed, "A comprehensive review of dimensionality reduction techniques for feature selection and feature extraction," *J. Appl. Sci. Technol. Trends*, vol. 1, no. 1, pp. 56–70, May 2020.

[46] D. Sun, J. Wu, J. Yang, and H. Wu, "Intelligent data collaboration in heterogeneous-device IoT platforms," *ACM Trans. Sensor Netw.*, vol. 17, no. 3, pp. 1–17, Aug. 2021.

[47] J. Brownlee, *Data Preparation for Machine Learning: Data Cleaning, Feature Selection, and Data Transforms in Python*. Vermont, VIC, Australia: Machine Learning Mastery, 2020.

[48] D. Mustafa Abdullah and A. Mohsin Abdulazeez, "Machine learning applications based on SVM classification a review," *Qubahan Academic J.*, vol. 1, no. 2, pp. 81–90, Apr. 2021.

[49] E. H. Houssein, M. A. Mahdy, D. Shebl, A. Manzoor, R. Sarkar, and W. M. Mohamed, "An efficient slime mould algorithm for solving multi-objective optimization problems," *Expert Syst. Appl.*, vol. 187, Jan. 2022, Art. no. 115870.

[50] J. Chen, H. Jing, Y. Chang, and Q. Liu, "Gated recurrent unit based recurrent neural network for remaining useful life prediction of nonlinear deterioration process," *Rel. Eng. Syst. Saf.*, vol. 185, pp. 372–382, May 2019.

[51] D. Chicco and G. Jurman, "The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation," *BMC Genomics*, vol. 21, no. 1, pp. 1–13, Dec. 2020.

ABDULRAHMAN A. ALSHDADI received the Ph.D. degree in cloud computing from the University of Southampton, Southampton, U.K., in February 2018. He is currently an Associate Professor in computer science with the College of Computer Science and Engineering, University of Jeddah. His research interests include industry 4.0 presenting issues of cloud computing and fog computing security, the Internet of Things (IoT) and smart cities, intelligent systems, deep learning, data science analytics, and modeling. He has published numerous conference papers, journal articles, and one book chapter. He was also awarded two patents from USPO, in 2021.

ABDULWAHAB ALI ALMAZROI received the M.Sc. degree in computer science from the University of Science, Malaysia, and the Ph.D. degree in computer science from Flinders University, Australia. He is currently an Associate Professor with the Department of Information Technology, College of Computing and Information Technology at Khulais, University of Jeddah, Saudi Arabia. His research interests include parallel computing, cloud computing, wireless communication, and data mining.

EESA ALSOLAMI received the degree in computer science from King Abdulaziz University, in 2002, and the M.Sc. and Ph.D. degrees in IT from the Queensland University of Technology, in 2008 and 2012, respectively. He is currently a Professor of computer science and engineering with the University of Jeddah. He is also the Dean of Admission and Registration at the University of Jeddah. His research projects involve feature selection techniques for continuous biometric authentication.

NASIR AYUB (Member, IEEE) received the Ph.D. degree in computer science from the School of Electrical Engineering and Computer Science (SEECS), National University of Science and Technology (NUST), Islamabad. Previously, he was a Lecturer at FUUAST Islamabad and a Senior Lecturer at CUST University Islamabad. He is currently a Faculty Member with the Department of Creative Technologies, Air University, Islamabad, Pakistan. His research interests include smart grids, machine learning, deep learning, natural language processing, and blockchain. He actively contributes to the academic community as a reviewer for IEEE Access, Elsevier, MDPI, and peer-reviewed journals. Furthermore, he serves as an Academic Editor for *PLOS One* and other scholarly journals.

MILTIADIS D. LYTRAS (Member, IEEE) is currently a Visiting Researcher at Effat University, where he contributes his expertise in various domains. Renowned as a world-class authority in cognitive computing, information systems, technology-enabled innovation, social networks, computers in human behavior, and knowledge management, he brings a wealth of experience to his roles as an editor, a lecturer, and a research consultant. His extensive background spans academia and the business sector across Europe and Asia. He has co-edited over 110 high-impact factor special issues in ISI/Scopus indexed journals and contributed to the co-editing/authoring of more than 80 books with international publishers, such as Elsevier, Emerald, IGI-Global, and Springer. Furthermore, he has co-edited over 100 peer-reviewed volumes/books on topics aligned with his expertise, covering subjects, such as digital transformation in healthcare, smart cities, and smart villages in the EU and beyond. His extensive contributions reflect his commitment to advancing knowledge and innovation across various disciplines. In addition, he has co-authored over 120 papers in Q1 and Q2 Web of Science and Scopus indexed journals, including prestigious publications, such as IEEE Transactions on Knowledge and Data Engineering, *Journal of Business Research*, and *Computers in Human Behavior*. He possesses 25 years of experience in research and development projects, demonstrating notable skills in conceptualization, financing, and implementation. His involvement in more than 70 research and development projects across Europe, the Middle East, and the Far East underscores his profound expertise. With a distinguished career, he has served as the Editor-in-Chief for the *International Journal in Semantic Web and Information Systems*. Throughout his career, he has held numerous senior editorial positions in esteemed journals, including the Editor-in-Chief and an Associate Editor roles. He has also guest-edited more than 130 special issues in high-impact factor journals. Notable among his editorial contributions are his roles as the Founding Editor and the Editor-in-Chief of journals, such as the *International Journal on Technology Enhanced Learning* and *International Journal of Knowledge Society Research*.