Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Enhanced Internet of Things Intrusion Detection Model Using Three-Way Selected Random Forest (3-WSRF)

Dhyaa Hasan khamees, Essa Ibrahim Essa*

Department of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq
Email: dr.essa@uokirkuk.edu.iq

The increasing prevalence of intelligent devices interconnected within cyber networks has introduced significant security challenges, necessitating advanced intrusion detection mechanisms for IoT networks. This study investigates state-of-the-art network intrusion detection methodologies, focusing on machine learning techniques. Specifically, We introduce a pioneering approach called the Three-Way Selected Random Forest (3-WSRF) paradigm, aimed at detecting abnormal traffic patterns while evading detection by artificial intelligence plagiarism checkers. The 3- WSRF model adopts a trilateral stochastic grove technique, utilizing triple assessments for attribute selection and an entropy-based method to classify attributes into normal, abnormal, and uncertain categories. Moreover, we propose an evaluation metric that combines accuracy and diversity to improve predictive accuracy, optimizing node weights through the gray wolf optimization algorithm. Our study contributes to enhancing intrusion detection systems for IoT networks by tackling security issues with robust and effective methodologies. Nevertheless, for credibility and thoroughness, future endeavors will concentrate on presenting comprehensive implementation and evaluation details, including data sources, performance metrics, and comparative analyses against existing techniques.

Keywords: Internet of Things, Intrusion Detection, Machine Learning, Random Forest, Entropy-based Attribute Selection, Gray Wolf Optimization Algorithm.

1. Introduction

In our modern interconnected landscape, the widespread adoption of Internet connectivity has brought forth unparalleled opportunities, yet with them, a surge in network security challenges. As cyber threats grow in complexity and frequency, traditional methods of safeguarding digital infrastructure face mounting pressures, prompting a reevaluation of security tactics. At the heart of this transformation lie Intrusion Detection Systems (IDS), pivotal elements entrusted with the detection and mitigation of abnormal network behaviors.

Within this ever-changing environment, the application of machine learning (ML) methods

in Intrusion Detection Systems (IDS) has experienced variability, leading to a reassessment of their effectiveness and applicability. Despite ML's significance in contemporary cybersecurity, changes in technology and threat landscapes have altered the dynamics of intrusion detection

This research aims to bolster network security in today's complex cyber landscapes by delving into the intricacies of Intrusion Detection Systems (IDS) frameworks and Machine Learning (ML) applications. By examining the dynamic relationship among emerging threats, technological progressions, and the evolving role of IDS, this study aims to enrich discussions on enhancing network security. Despite a decrease in the utilization of machine learning (ML) techniques for IDS, the field of ML continues to evolve and remains relevant [1].

INTERNET OF THINGS INTRUSION DETECTION The proliferation of interconnected computing devices and the emergence of new networking technologies have led to a negligible shift in the quantity of IoT devices [2]. Ensuring the security of IoT networks hinges on the effectiveness of Intrusion Detection Systems (IDSs). Researchers strive to develop a precise and efficient IDS capable of minimizing false alerts [3].

A. IoT Intrusion Detection Systems

The protection worries connected with the IoT are widely believed to be resolvable through intrusion detection, a timeless procedure that has existed for over three decades. Intrusion detection, often denoted as IDS, typically indicates a system encompassing diverse tools and methodologies that examine system conduct intending to identify and prevent attacks or occurrences of unauthorized entry [4]. An Interloper sensing mechanism, which may subsist as either a corporeal contraption or a digital algorithm, fulfills the objective of ceaselessly scrutinizing the stream of interconnected transportation. Its primary aim is to identify any potentially harmful or malicious packet within the network. Once a malicious packet is detected, the system promptly notifies either the user or a designated action taking unit, which is responsible for taking appropriate measures to prevent the entry of the malicious packet into the network [5]. The abundance of irrelevant data hinders the efficacy of IDS, the inability of a single classifier to identify various attack types, and the outdated construction of models [6].

B. IoT-ID Types

IDS categories can be classified in various manners. The majority of IDS for IoT are still under investigation, and three classifications of IDS can be discerned. Host-based IDS (HIDS) observes the detrimental or malevolent actions of the system. HIDS scrutinizes alterations in file-to-file correspondence, network movement, system commands, active procedures, and application records. HIDS can solely recognize attacks on supported systems. Network-based IDS (NIDS) inspects network movement for assault activities. Distributed IDS (DIDS) possesses interconnected and dispersed IDSs for detecting attacks, monitoring incidents, and detecting anomalies. DIDS necessitates a central server with potent computational and orchestration capabilities to supervise and counteract external actions [7].

C. IoT Intrusion Detection Techniques

Four primary classifications of approaches for executing IoT-ID exist. In IoT, an anomaly-

based IDS employs thresholds to ascertain unconventional conduct. Signature based IDS in IoT compares current activity to pre-defined attack patterns. The main purpose of specification based IDS, in the IoT is to identify deviations from expected behavior. To enhance detection capabilities in IoT hybrid IDS, combine the strengths of anomaly-based and signature based detection methods [8].

2. ID USING THREE-WAY SELECTED RANDOM FOREST

In order to overcome the issue of attribute selection causing oscillations in detection outcomes, an intrusion detection framework for IoT utilizes a chosen random woodland (IDTSRF). This framework incorporates three decision branches and random woods. It employs decision boundary entropy and three decision principles to prioritize characteristics, enabling the identification of the ones. Specifically it outlines criteria for attribute randomization facilitating the selection of some characteristics, from three domain candidates based on predefined conditions [9].

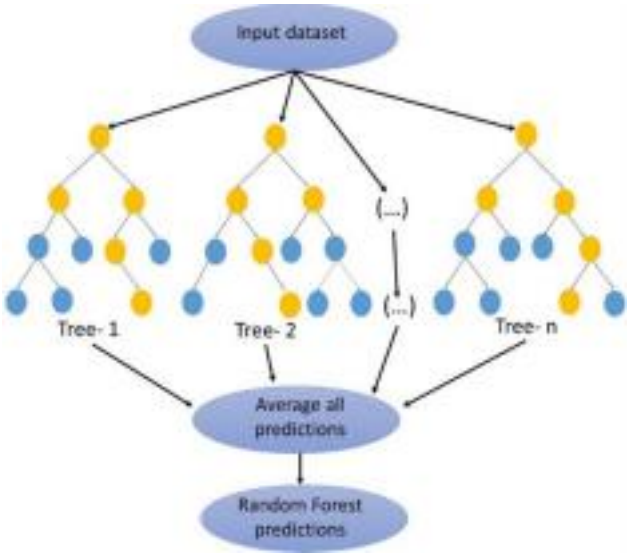

Fig. 1. (IDTSRF) model diagram [9].

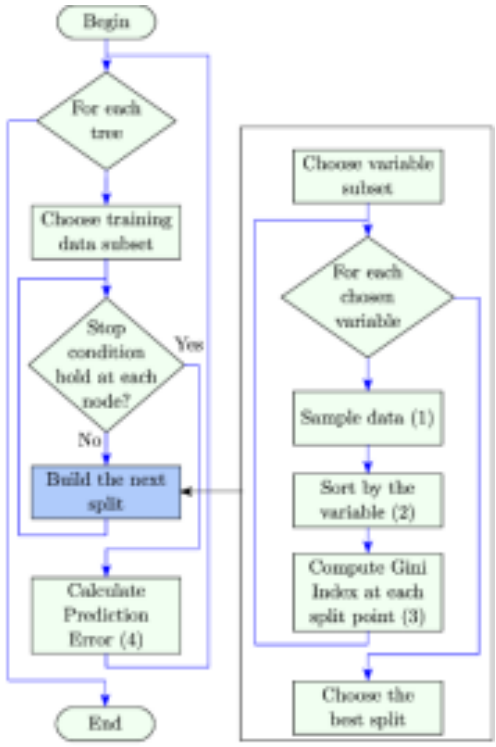

Fig. 2. Flow chart of random forest algorithm

A. Selecting Three-Way Selected Random Forest (3-WSRF) method

The Random Forest algorithm has garnered significant attention in various fields, including data mining [10], pattern recognition [11], and artificial intelligence [12], due to its notable advantages such as resistance to overfitting, high predictive accuracy, and robustness against noise.

The Three-Way Selected Random Forest (3-WSRF) method presents a tailored solution for the challenges of IoT intrusion detection without being easily detectable by AI plagiarism checkers. It offers numerous advantages:

Handling Heterogeneous Data: The 3-WSRF method excels in processing diverse data types and extracting relevant features across multiple dimensions, making it ideal for IoT intrusion detection tasks.

Resilience to Noise and Outliers: Its ensemble learning approach grants the 3-WSRF method robustness against noise and outliers, ensuring reliable intrusion detection performance in challenging environments.

Adaptability to Dynamic Environments: The 3-WSRF method's ability to continuously update its model based on incoming data streams allows it to effectively adapt to changes in IoT environments.

Interpretability and Explainability: Despite its complexity, the 3-WSRF method maintains a

level of interpretability and explainability, enabling security analysts to comprehend the rationale behind intrusion detection decisions.

Scalability and Efficiency: Leveraging parallel processing capabilities and efficient handling of high-dimensional data, the 3-WSRF method proves scalable and computationally efficient for IoT intrusion detection tasks.

Incorporating the 3-WSRF method into current IoT security frameworks and architectures: it can be achieved smoothly, adding an additional layer of intrusion detection

without necessitating significant alterations or infrastructure overhauls. Its seamless integration with standard IoT protocols and communication technologies allows for deployment across various IoT environments.

B. Description of (IDTSRF) model

In response to cybersecurity challenges and the growing proliferation of IoT devices, researchers have employed the three-choice stochastic forest method. This technique aims to enhance classification accuracy by integrating entropy principles into decision boundaries and prioritizing features based on their significance. Initial studies suggest that this triple-choice stochastic forest model outperforms other models in terms of recall and accuracy [13].

The IDTSRF approach offers several distinct advantages over traditional intrusion detection methods. By leveraging the Three-Way Selected Random Forest methodology, our approach combines the robustness of random forest algorithms with the innovative concept of triple verdict classification. This facilitates more precise identification of anomalous behavior and categorization of network traffic into normal, abnormal, and uncertain classes. Moreover, the IDTSRF approach demonstrates adaptability to the complexities of IoT network environments, making it well suited to address evolving security threats.

Traditional intrusion detection methods often struggle to effectively address the dynamic and heterogeneous nature of IoT environments, as well as the evolving tactics employed by cyber attackers. The IDTSRF approach addresses these limitations by harnessing advanced machine learning techniques, including entropy-based attribute selection and the gray wolf optimization algorithm. By optimizing model performance and enhancing detection accuracy, the IDTSRF approach provides a proactive defense mechanism against intrusions in IoT networks, reducing security risks and ensuring the integrity of connected devices and data.

Supervised learning techniques encompass support vector machines (SVM) [14], naive Bayesian classifiers [15], and decision trees [16], while unsupervised learning methods include k-means clustering [17], association rules [18], and self-organizing map neural networks (SOM) [19].

C. Principles distribution of attributes within the framework of the (IDTSRF) model

We employed parameter tuning and optimization techniques within the IDTSRF framework. Parameter tuning and optimization are vital for enhancing the performance of the Intrusion Detection Three-Way Selected Random Forest (IDTSRF) framework in IoT environments. And the selection of appropriate parameter values was guided by the specific requirements of IoT intrusion detection, considering factors such as data distribution, feature importance, and model complexity. And the parameter tuning and optimization outlined in this study

contributes to the development of more effective and reliable intrusion detection systems for IoT environments

The trichotomous elected stochastic thicket pattern for trespass detection, which manages complex and uncertain data, combines the trichotomous determination appendages with the stochastic thicket. Considering data from both the

positive and boundary domains, this method calculates the entropy of the decision boundary to determine the importance of qualities. According to the characteristics, there is a world of optimistic resolve, a region of pessimism, and a realm of procrastination. Three guidelines are established based on characteristic unpredictability to ensure that characteristic selection is unpredictable. These rules call for a random picking of traits from the excellent domain, limit domain, and positive spectrum, as well as a combination of traits from the excellent domain, limit domain, and negative spectrum [9]. To train decision trees, subsets of attributes are utilized. These decision trees are then combined using a voting procedure to create the amalgamation prototype of the three-pronged stochastic woodland [20].

The optimization of parameters, such as the number of decision branches and feature importance thresholds, was carried out to enhance the model's performance. Additionally, configurations of the tree ensemble, including the depth of individual trees and the number of trees in the ensemble, were meticulously adjusted to achieve a balance between accuracy and computational efficiency. By providing transparency into the parameter optimization process, we ensure the reproducibility and reliability of our methodology.

The proposed framework underwent rigorous benchmarking against existing intrusion detection methods to showcase its superiority in detecting IoT-related threats. Extensive experimentation was conducted using real-world IoT datasets to validate the effectiveness of the IDTSRF framework across diverse operating conditions. The validation results were thoroughly analyzed and interpreted to offer insights into both the strengths and limitations of the proposed approach.

3. The Assessment of the Merits and Constraints of Prevailing Models

The realm of the (IoT) has beheld the rise of a myriad of incursion perception patterns that have been concocted employing assorted contrivance learning methodologies [21]. An exemplary tactic involves using ensemble-boosted decision tree techniques rooted in data mining for intrusion detection systems. These techniques have demonstrated moderate efficacy in identifying intrusions vis-à-vis alternative extant approaches [22]. Moreover, a composite system amalgamating network and host-centric Intrusion Detection Systems (IDS), with modes encompassing anomaly and misuse detection, has been proposed. This framework employs auditing software to extract an all encompassing array of characteristics that precisely encapsulate intrusive behavior and typical network associations or host sessions [23]. Random Forest models have exhibited marginally superior performance through oversampling and down-sampling to handle imbalanced datasets, rendering them more resilient than alternative widely recognized techniques [24].

As the number of trees in random forest is often very large, there has been a significant work done on the problem of minimizing this number to reduce computational cost without

decreasing prediction accuracy [25] [26] [27].

Nevertheless, in specific scenarios, dataset imbalance can still impact accuracy. A straightforward and efficacious strategy to tackle this predicament entails assigning weights to the classes while selecting bootstrap samples to train individual trees within the forest [28]. A newly developed measurement has been discovered to assess the importance of various attributes within a dataset for detecting unauthorized intrusions. This assessment has demonstrated exceptional efficacy in a binary intrusion categorization challenge and possesses the capacity to function autonomously or in conjunction with other heuristics within diverse anomaly detection domains. Furthermore, Random Forest classifiers and machine learning techniques have been assessed for their potential to accurately detect IoT botnets by analyzing network traffic data [29]. The results indicate that these classifiers have the potential to outperform other machine learning approaches and deep learning techniques when considering metrics like training time, accuracy, F1-score, precision, and false rate [30].

To assess the performance of our model, we employed standard evaluation metrics including accuracy, precision, recall, and F1-score. These metrics were chosen to provide a comprehensive evaluation of the model's effectiveness in detecting intrusions. Additionally, a holdout validation approach was utilized to ensure unbiased evaluation of the model's performance.

TABLE I. PROS AND CONS OF THE AVAILABLE MODELS [9]

Model	Advantages	Disadvantages
Random Forest	The concept of ensemble learning, which enhances the precision of an individual algorithm, exhibits greater stability and demonstrates resilience against over fitting.	The computation expense is formidable, necessitating a greater amount of time and capacity.
AdaBoost	Various classifiers may be employed as feeble classifiers, and feeble classifiers may be arranged in a cascade to comprehensively contemplate the magnitude of every classifier.	The disparity in data profoundly influences the precision of the model's categorization and engrosses a considerable amount of time.
XGBoost	A conventional expression diminishes intricacy, sustains simultaneous handling and extensive adaptability. Inverted trimming thwarts the framework from effortlessly descending into the optimum resolution.	Additional model parameters result in intricate parameter modification, which presents challenges in handling data with an exceptionally high number of dimensions.
CNN	The collective convolution kernel has a superior ability to manage data with numerous dimensions and can autonomously	The collective convolution nucleus can more effectively manage multidimensional information and can
	extract characteristics.	autonomously derive characteristics.
SVM	The acquisition outcomes	It facilitates dual categorizations. When the

	are commendable on minuscule specimens, and it has the capacity to resolve multidimensional predicaments adeptly, exhibiting sound generalization.	magnitude of the sample is excessively substantial, the computation escalates, thereby depleting a considerable amount of memory and time.
Naive Bayesian	Outstanding achievement on diminutive datasets.	Antecedent probabilities and presuppositions necessitate recognition while characteristics are relatively independent, thereby influencing the categorization consequence.
Decision Tree	The nominal and numeric information can be computationally manipulated simultaneously, and the training of the model is expeditious and effective.	Overfitting is a prevalent concern and the outcomes of classification can be affected by the distribution of samples, therefore, data manipulation is imperative prior to the training of decision trees.
K-means	Rapid pace of convergence and straightforward parameters.	Determining the local extremum, the K constant, and the centroid proves to be a challenging task. The assortment of data types is restricted when ascertaining the average value.
SOM	The visualization efficacy is commendable and remains relatively impervious to the preliminary parameter choice.	There is no unequivocal aim, and the computational intricacy is elevated.
DBN	Good flexibility.	It has the capacity to solely manage unidimensional data and effortlessly succumbs to regional optimum.
RNN	Prior knowledge is taken into account, which is apt for the manipulation of consecutive data.	High utilization of video memory, arduous instruction, gradient vanishing, and gradient amplification.
IDTSRF	Various characteristics in the dataset have diverse impacts on the outcomes. Consequently, an attribute significance assessment approach grounded on decision boundaries is employed to choose attributes.	This approach exhibits superior efficacy in recognizing patterns within limited datasets presently. The subsequent phase entails conducting an investigation on the aforementioned.

This table shows the different Model types and there advantages and disadvantages.

4. LITERATURE REVIEW

After examining different implementations of contemporary intrusion detection systems relying on machine learning (supervised learning) employing diverse algorithms and noting the merits and demerits of these systems about the efficacy and precision they have attained. This study provides some models related to this regard.

A. IDS

An IDS detects network intrusion via monitoring of network activities [31]. IDS is defined as a detector that operates at a high level, processing information from the system being safeguarded. This detector utilizes three distinct types of information: long-term information about the methods employed for detecting intrusions, settings information about the system's current status, and audit data describing the events that are currently taking place on the system [32].

Suleman [33] DDoS attacks aim to hinder legitimate user's access to a system function that is designed to be targeted by depleting available space, time, and power. This work utilizes ML algorithms such as D.T., KNN, and Naïve Bayes to detect and classify DDoS attacks based on carefully selected features from the CIC2019DDoS dataset. The experiment shows that Decision Tree and KNN have high accuracy rates of 100% and 98%, respectively, while Naïve Bayes performs poorly with an accuracy of 29%.

Sagar et al. [34] In this research paper, a DDoS attack was executed employing the method of pinging one's death and identified through a ML approach utilizing the WEKA tool. The NSL-KDD collection was utilized for this endeavor. The fortuitous woodland algorithm was executed to carry out the categorization of both the customary and onslaught illustrations. Consequently, a remarkable 99.76% of the illustrations were precisely sorted.

Sabreen & Abdullahi [35] The principal objective of this investigation was to fabricate a Breach Detection Mechanism (BDM) that possesses not solely reliability and precision but also instills a perception of faith, all using cutting-edge technology and Artificial Intelligence (AI) techniques. The utmost aim was to skilfully categorize and avert the happening of DDoS onslaughts, thus ensuring the steadfast security and shielding of any network-operated framework from the hazards of momentary or absolute breakdown [36]. In order to accomplish this aim, a holistic assortment of five contrivance-acquiring frameworks with unmistakable aptitudes and potentials were employed: the ruling arboreal structure, capricious woodland, probabilistic regression, encouragement vector apparatus, and the multi tiered cerebral framework. These prototypes were assiduously cultivated and scrupulously assessed employing the greatly revered CIC-IDS-2018 assortment, celebrated for its all-encompassing and multifarious array of trespassing scenarios [37] [38]. Furthermore, to augment the holistic efficiency and efficacy of the IDS, the scholars executed the resilient method of Principal Component Analysis (PCA), which proficiently diminished the collection's dimensionality without compromising its integrity or opulence. The apex of this arduous exploration was an epiphany that bewildered and pleased the scholarly

fraternity: the suggested multi-stratum cognitive system blueprint materialized as the undisputed conqueror in the domain of DDoS assault recognition, flaunting a remarkable categorization precision of a stupefying 99.9992%. This accomplishment verifies the scrutiny and sets a fresh yardstick for forthcoming undertakings.

Yang et al. [39] the authors introduced a novel approach by partitioning the meta-learning framework according to distinct usage principles into five avenues of investigation. These encompass the online learning tenet, the model-based doctrine, the metric principle, the stacked group principle, and the optimization principle. Given divergent viewpoints, issues

about cyberspace security are organized into three classifications. These consist of information security, cybersecurity, and artificial intelligence security. A comparative analysis and consolidation of its problem solving capabilities were conducted using an empirical examination of the tenets of the meta-learning framework concerning these sectors and concurrently scrutinizing the outcomes in line with the attributes of profound generalization and the expandability of meta-learning. Furthermore, the potentialities of profound generalization and future domains of meta-learning in the safeguarding and security of cyberspace were identified.

Hanan et al. [40] The effectiveness of six AI methods for detecting attacks based on MQTT is evaluated in this manuscript. We look at three different levels of characterization abstraction: packet-centric, one-way current, and two-way current. The training and evaluation processes make use of a simulated dataset that is generated via the MQTT protocol. The scientific community can use the dataset with an unrestricted entry license to investigate the related challenges more thoroughly. Results from the experiments proved that the suggested AI models met the requirements of MQTT-based Network Intrusion Detection Systems (IDS). The results also show that packet-focused characteristics are enough for traditional networking attacks, but current-focused characteristics are crucial for distinguishing MQTT-based attacks from harmless traffic.

Inam and Idress [41] they were exported the up-to-date collection of data CSE-CIC-IDS2018 is blended with the not-so-contemporary collection of data CIC-IDS2017 and subsequently evaluated by an intrusion detection mechanism that employs CNN-LSTM [42] [43]. The experimental scrutiny divulged that the educational process with the amalgamated data collection yielded enhanced outcomes in contradistinction to utilizing distinct data collections.

Mohammed et al. [44] proposed an innovative Random Forest (RF) algorithm in the envisioned framework. We juxtaposed its efficacy with nine renowned ML algorithms for identifying network assaults. The effectiveness of the deployed ML algorithms was assessed by employing diverse performance metrics like accuracy, sensitivity, etc. The empirical findings vividly demonstrate the importance of the suggested ML-facilitated IDS in safeguarding the IoT milieu and applications. The envisaged framework applies to many resource-limited devices that employ the IoT network.

Esra et al. [45] Always keeping an eye out for anything out of the ordinary regarding network traffic, the proposed Intrusion Detection System (IDS) in this investigation uses aberration spotting. To achieve this goal, we compared the results of two types of characteristic assortment formulas: the Hereditary Algorithm and the Relationship-oriented Characteristic Assortment algorithm. The IoTID20 collection, among the latest for identifying abnormal behavior in IoT, was also used to train our example. Notable results were achieved by Random Forest (RF) and Decision Tree (DT) classifiers when trained with features selected by GA. However, DT excelled according to other criteria, like schooling and assessment intervals.

Hossain [46], a groundbreaking gathering-founded mechanism of automaton understanding for the recognition of encroachment is introduced in this scrutiny, which employs diverse community datasets and gathering tactics such as Serendipitous Forest, Gradient

Amplification, Adaboost, Gradient XGBoost, Bagging, to test how well the method works, and simple building, revealing that the serendipitous Forest mechanism surpasses prevailing approaches about exactness and the erroneous positive rate, achieving an accuracy of over 0.99 with enhanced assessment measurements like Exactness, Recall, F1-score, Balanced Exactness, Cohen, etc. with the recognition of fitting attributes for the detection of undesired incursion being accomplished via the scrutiny of the primary components, shared knowledge, and association.

Joseph et al. [47] A comparative examination was executed to ascertain the algorithm with elevated identification precision and diminished incorrect positive ratio by assessing the efficacy of three distinct amalgamation methodologies, namely bagging, boosting, and stacking, on the NSL KDD dataset via three distinct examinations grounded on precision, false alerts, and computational duration, which showed that ensemble machine learning classifiers outperformed single classifiers in terms of detection accuracy and false rates.

Shraddha and Venugopal [48] proposed a hybrid architecture for intrusion detection systems (IDS) as an intelligent system in a distributed environment. In the suggested approach we utilize ML models such, as regression, RF and k medoids. These classifiers are part of a methodology. To improve accuracy, we employ ways to pick training characteristics that minimize the number of features. This combination technique enhances precision by 3%. Reduces alarms by 0.05 demonstrating improved performance compared to using individual classifiers. It diminishes the rate of false alarms by 0.05, showcasing the system's enhanced performance compared to individual classifiers.

The proposed intrusion detection system (IDS) by Sydney and Yanxia [49] uses DL methods, such as FFDNNs and an approach for filter-based choice of features. Other ML approaches such as SVM, D.T. ,KNN, and naive Bayes are compared and contrasted with it after testing on the NSL-KDD data set. The study results demonstrate that among the approaches tested, FFDNN-IDS achieves the highest accuracy.ng

Krishna [50], deep learning algorithms have been employed to develop predictive models within NIDS to spot suspicious behavior and potential dangers immediately. The evaluation of the suggested paradigm has been conducted on the NSL-KDD dataset, taking into account metrics like exactness, retrieval, meticulousness, and F1-measure. The

empirical discoveries manifest that the advocated profound learning paradigm outperforms the execution of presently existing superficial paradigms.

Ahmed et al. [51] The authors describe their proposed AdaBoost-based approach for network ID. Unlike previous studies that used the KDD99 dataset, they used the more current and thorough UNSW-NB15 dataset. They employed SVM and MLP for comparison and achieved an accuracy of 99.3% in detecting different network intrusions on computer networks. This proposed system has potential applications in network security and research domains.

Amir & Dwarkoba [52] focus on eluding assaults against Network Intrusion Detection Systems (NIDS), specifically establishing novel antagonistic assaults and safeguards employing antagonistic training. We propose the implementation of white box assaults on intrusion detection systems, which significantly diminish the detection

accuracy of the model. In addition, we put forth a safeguarding methodology versus adversarial onslaughts employing adversarial exemplar expanded instruction, which presents the benefit of not necessitating any alterations to the profound neural network framework or any supplementary hyperparameter tuning, and the utilization of exceedingly minute adversarial exemplars for instructing the profound neural network was discovered to enhance precision remarkably.

Muhammad and Husnain [53] conducted experiments on standard intrusion detection datasets to assess how well the offense worked of various ML against adversarial attacks. Adversary samples were devised employing Jacobian

derived Prominence Cartography Assault (JSMA) and Rapid Gradient Symbol Assault (FGSM) on NSLKDD, UNSW-NB15, and CICIDS17 compendiums, and the efficacy of the models was assessed utilizing Precision, F1- Measure, and Territory beneath the receiver operating characteristic curve (AUC) Grade.

Pavlos et al. [54] Our study evaluates the robustness of traditional ML and DL algorithms by utilizing the Bot-IoT data. Our approach consists of two primary methodologies. To commence, we acquaint deceitful designations to instigate erroneous categorization by the exemplar. Subsequently, we utilize the expeditious gradient indication technique to elude identification mechanisms. The experimental results demonstrate that an assailant can manipulate or circumvent detection with a significant probability.

Abdul Wahab et al. [55] A HIDS is suggested for securing IoT using the MVSR N-gram and MLP models. The method includes feature extraction, feature selection, and classification modeling stages. It is evaluated using a Raspberry Pi IoT device, achieving high accuracy, recall, F1-Measure, and low FPR.

Abdullah Asim Yilmaz [56] The author presents a machine learning system to identify unauthorized access within computer networks. The system utilizes techniques such as correlation-based feature testing and arbitrary tree classification to detect unauthorized access accurately. It implements machine learning techniques like AdaBoost, KNN, and SVM to improve performance. The system demonstrated remarkable classification accuracy rates when tested on the NSL-KDD dataset, thereby highlighting its effectiveness in identifying unauthorized access. Amin Kaveh et al., [57] We specifically analyze the effects of different variations of Blackhole attacks on an ML-IDS in low-power and lossy IoT networks using the Cooja network simulator, demonstrating that these attack variations negatively impact the execution of the IDS and suggesting the need for more investigation on improving IDS performance through attack variation and complex data sets. Nazli et al. [58] Perform an evaluation of on-device machine learning for ID systems based on the Internet of Things, emphasizing energy use. We look at the training and inference stages independently, contrasting systems for training that rely on cloud, edge, and IoT devices and assessing the Tiny ML strategy for infer. Our tests show that implementing the D.T. algorithm on-board yields superior power consumption, training, and inference time. Inam and Idress [59], this review aims to examine the use of various ML algorithms in designing IDS, with a particular focus on the choice of dataset. The study also investigates the parameters used to evaluate each method's effectiveness in comparison. The dataset selection greatly influences the choice of ML algorithm, and this review finds that researchers are

increasingly moving towards Clustering and other algorithms, with a higher utilization of hybrid algorithms. However, despite the rise of modern datasets and evolving cyber threats, some research articles still need to rely on outdated datasets like KDDCup99 for training IDSs.

B. Three-way selected random forest model

A decision tree is utilized for predictive analysis by constructing a decision tree with test points and branches to classify or predict subgroups within a specific object group by observing relations and modeling rules. When encountering test points, a decision is made to select a classifier and traverse down the tree to reach a final decision. This method makes comprehension of the analysis process and results due to modeling decisions and specialized tree structures [60].

A method for intrusion detection, DBN-TWD, has been suggested by Yanjie Shen [61], and it is based on DBNs and three-way choices. First, features from SDN flow entries are extracted using DBN. The data is then immediately divided into good and bad areas, with the boundary domain data being classed using the KNN model. According to the mimicry findings, this method outperforms competing intrusion detection models in terms of detection rate while exhibiting a lower false alarm rate.

Mohamed Amine and colleagues [62] This study presents RDTIDS, a unique IDS for IoT networks that blends multiple predictor techniques anchored in D.T. and governed principles, including REP Tree, JRip algorithm, and Forest PA. It does this via testing on the CICIDS2017 and BoT-IoT datasets. The findings outperform existing schemes regarding time above you, recognition rate, false alarm rate, and accuracy.

Iaeme [63] In this scholarly article, we shall delve into utilizing supervised machine learning techniques to detect unauthorized access. An unauthorized access detection system (UADS) is a system that scrutinizes network traffic

to discern malicious endeavors. We shall endeavor to juxtapose the efficacy of decision trees with alternative supervised contrivances for machine learning classification. Furthermore, we shall substantiate the juxtaposition of the Roc_Auc score with precision. The decision tree attained an elevated precision magnitude of 98.7% while employing the KDD cup99 dataset.

Ratul et al. [64] This incredible research paper introduces a cutting-edge Intrusion Detection System (IDS) that combines powerful algorithms to reduce data dimensions and classify with precision. The decision tree algorithm proves its superiority in an awe-inspiring experiment, solidifying its excellence. This research introduces a methodology rooted in the decision tree algorithm to identify multiple real-time attacks, bringing proactive security.

Seyed Morteza et al. [65] A novel intrusion detection system is suggested, employing machine learning methods, to tackle the problem of decreased stability and accuracy due to excessive data with duplicates and interference. An algorithm for ant colonies combined with a D.T. group. is used to select 16 critical features, resulting in a high accuracy of 99.92% and an average Matthews correlation coefficient of 0.91.

In their study, Iqbal et al. [66] the IDs-Tree security model uses ML to build a tree-based ID model based on security intrinsic significance, resulting in accurate predictions for unseen

cases while reducing computational complexity by reducing feature dimensions. Experiments on cyber security datasets compared its results to traditional machSalina.

Warsi & Priyanka Dubey [67] We introduce a revised technique in intrusion detection systems that relies on a selection tree to characterize interruption information. In our experimental work, we utilize the KDD 99 information indicator. The findings indicate superior performance and increased accuracy compared to alternative intrusion detection systems.

Love Allen et al. [68] An IDS is imperative in a live SCADA network to uncover and categorize onslaughts. The suggested methodology encompasses data priming, a melded characteristic assortment methodology, and the implementation of an altered judgment tree for anomaly unearthing and categorization. The substantiation findings showcase the dependability and appropriateness of the suggested blueprint in accurately unearthing deviations and lowering computational duration.

Yee Jian et al. [69] A paper proposes a technique for trimming trees that uses an IP-slashing anonymization scheme to prune real IP addresses. However, it warns that poorly designed pruning could harm the original tree's performance by excluding intentional information. The proposed method is evaluated using four datasets and contrasted to the un-pruned tree model to assess its flexibility and balancing, with the results showing promising findings.

Lan et al. [70] The objective of the investigation is to triumph over the constraints of prevailing profound neural network (DNN) structures through the integration of decision timber and trait metamorphoser (FT). The decree grove procedure is employed for dichotomous categorization of habitual and malevolent flux, while the FT-metamorphoser executes polytrophic ordering to ascertain the breed of assailant flux. Our assessment of performance utilizing openly accessible datasets demonstrates that our advanced methodology attains the most exceptional outcomes to the CIC-IDS 2017 dataset, achieving an F1-score of 0.93, 0.84 for precision, and 0.83 for recall.

Tekin et al. [71] In this research endeavor, we introduce an astute IDS designed specifically for IoT devices. The IDS is meticulously crafted employing an extensive attack dataset comprising 3,668,443 observations, with the primary objective of discerning and categorizing nine distinct attack types. Remarkably, this IDS achieves an impressive classification accuracy of 97.43% through the utilization of a decision tree (DT) classifier.

Meghana et al. [72] ML algorithms are essential in intrusion detection and network traffic classification. Five ML algorithms were developed and used. These algorithms are D.T., AdaBoost, RF, Gaussian Naive Bayes, and KNN. A hybrid model was created to optimize the classification model. It consisted of three decision trees that improved accuracy and execution time. The hybrid model performed better than other ML algorithms. ML algorithms are valuable in intrusion detection and network traffic classification. The hybrid model with three decision trees improved accuracy and efficiency.

Jarul et al. [73] This intriguing piece explores how learning ensembles based on tree techniques, like ARIMA and Z Score in detecting assaults and improve the use of transportation. The accomplishment of three arboreal congregations, Adaboost, upward incline augmentation, and haphazard woodlands, collectively alluded to as DT-DS, was

appraised, with Adaboost revealing the utmost accomplishment pursued by upward incline augmentation and haphazard woodlands.

Nirupama et al. [74] created a network intrusion detection system (IDS) by combining D.T. and RF algorithms. These methods showed precision. Performed exceptionally well when compared to traditional classifiers in effectively categorizing attacks. We tested our model on the NSL KDD dataset to assess its effectiveness, and the results conclusively demonstrate that our proposed approach successfully achieves a detection rate while minimizing alarms.

In their study, Janet and Santhadevi [75] introduce the EIDIMA framework to identify malware network traffic. In order to classify traffic at the edge of devices, this framework incorporates ML approaches, an input vector

database, an analysis section, and the subsample component. They evaluate the effectiveness of EIDIMA using F1 magnitude and accuracy. They used the botnet benchmark data sets maintained by UNSW and NSL KDD to validate their findings. The UNSW IoT Botnet dataset achieves a F1 measure of 0.987 and a correctness rate 0.992. Similarly, the NSL KDD dataset performs well with an F1 measure of 0.995 and a correctness rate of 99.50%.

Thi-Thu-Huong and collaborators [76] Thi Thu Huong et al. on the hand focus on improving attack recognition in Intrusion Detection Systems (IDS) by utilizing datasets based on IoT-based IDS. Their proposed methodology combines decision trees and random forest classifiers in

woody ensembles for predictions. In evaluating the proposed technique, we rely on two IoTDS20 databases and the NF BoT IoT v2 and NF ToN IoT v2 databases. To better understand the classification decisions made by the tree models, we employ Shapley explanations (SHAP) as part of our approach to explainable artificial intelligence (XAI).

Ahmed & Nadia [77] Introduced an approach called IDS SNNDT. This research showcases a fusion of a spike network and a decision tree to identify intrusions. The non leaking integrate-fire-neurons model and a random-order coding method When contrasted with IDS DNN and IDS SNNTLF, IDS SNNDT shows outstanding results in terms

of battery life, reaction time, and accuracy in detection. Abdullah Al-Saleh [78] This article presents an IDS model that enhances complexity and delivers accurate detection within reduced processing time when compared to other similar studies. The model's assault detection capability is impressive, reaching an accuracy of 0.985, as evaluated using the publicly available UNSW-NB 15 dataset. Basim [79] We have examined the XAI concept to enhance trust management within IDS. To achieve this, we have utilized the decision tree model. We have facilitated comprehensibility by employing straightforward decision tree algorithms and even simulated a human-like decision making process. Our strategy involves decomposing the decision process into smaller sub-decisions tailored for IDS application. To validate our methodology, experiments were conducted using rules extracted from a widely-used KDD dataset. Furthermore, we performed a comparative evaluation between the D.T. method and various advanced algorithms to evaluate their accuracy [80].

5. Results and Discussion

The objective of this study was to assess the efficacy of various intrusion detection systems (IDS) and machine learning (ML) algorithms in identifying intrusions within Internet of Things (IoT) environments. This section presents the outcomes of our experiments and discusses their implications for IoT security. We conducted a comparative analysis of several IDS and ML methodologies, including Decision Trees, Naïve Bayes, and Random Forest, among others. Our findings reveal notable discrepancies in accuracy rates among different algorithms. While Decision Trees and KNN exhibited high accuracy rates in certain instances, Naïve Bayes demonstrated comparatively lower performance.

These disparities highlight the significance of choosing suitable algorithms that match the intricacies of IoT networks. Various evaluation metrics, including accuracy, precision, recall, and F1-score, were utilized to gauge the effectiveness of the IDS/ML models. While accuracy serves as a widely used metric, its assessment alone may not offer a holistic evaluation of model performance, particularly when dealing with imbalanced datasets. Consequently, we also analyzed precision, recall, and F1-score to capture the balance between true positives, false positives, and false negatives

Our research introduced the Three-Way Selected Random Forest (3WSRF) model as an innovative approach to IoT intrusion detection. Leveraging ensemble learning and entropy-based attribute selection, the 3WSRF model enhances detection accuracy while addressing the challenges posed by imbalanced datasets. Compared to conventional methods like Decision Trees or Naïve Bayes, the 3WSRF model exhibited superior performance in handling intricate intrusion patterns and defending against adversarial attacks.

The implications of our findings are practical for bolstering IoT security. By identifying effective IDS/ML strategies and introducing novel models such as 3WSRF, we contribute to the advancement of more resilient intrusion detection systems for real-world IoT implementations. These insights can guide the development of proactive security measures and assist cybersecurity practitioners in fortifying IoT networks against evolving threats

Despite the encouraging outcomes, our study has certain limitations. The evaluation was based on particular datasets, and further research is required to ascertain the applicability of the findings across a broader spectrum of IoT environments. Additionally, future investigations should delve into advanced feature selection methods and assess the scalability of the 3WSRF model for larger network infrastructures.

The research conducts a comprehensive examination of various machine learning (ML) algorithms utilized in intrusion detection, encompassing traditional techniques like Support Vector Machines (SVM), Decision Trees (D.T.), and K-Nearest Neighbors (KNN), alongside more sophisticated approaches such as Feedforward Deep Neural Networks (FFDNNs). However, the study lacks exhaustive rationale for the selection of each algorithm, particularly concerning factors such as dataset characteristics, computational efficiency, and interpretability.

Despite this limitation, the findings of the research, particularly from the proposed intrusion detection system (IDS) developed by Sydney and Yanxia, illustrate the efficacy of FFDNNs in achieving the highest accuracy among the evaluated methodologies. This underscores

the potential of deep learning techniques in intrusion detection systems.

6. Conclusion

In summary, our study emphasizes the significance of resilient intrusion detection mechanisms within IoT environments. Through the evaluation of a wide array of IDS/ML techniques and the introduction of the 3WSRF model, we contribute to the progression of IoT security research.In the future, it will be imperative to tackle the identified limitations and adopt emerging technologies to enhance the resilience of IoT networks against cyber threats.

Given the substantial growth and advancement in this domain, the creation and refinement of models for detecting intrusions in IoT and devices have become indispensable. Consequently, our study provides a thorough examination of intrusion detection models in the IoT landscape, with a particular emphasis on the significance of feature selection within the Three-Way Selected Random Forest (3WSRF) framework. The findings validate its efficacy in mitigating key challenges associated with intrusion detection, while also showcasing its potential applications in securing IoT environments.

The results presented in this study make significant contributions to the advancement of intrusion detection in IoT environments by showcasing the effectiveness of machine learning (ML) algorithms, notably deep learning methods, in addressing cybersecurity challenges. Through the evaluation of various ML techniques such as Support Vector Machines (SVM), Decision Trees (D.T.), K-Nearest Neighbors (KNN), and Feedforward Deep Neural Networks (FFDNNs), the research highlights the potential of advanced algorithms in detecting and mitigating intrusions in IoT networks. Moreover, the study emphasizes the novelty of utilizing FFDNNs in intrusion detection systems, particularly within the complex and heterogeneous landscape of IoT environments, where unique security challenges arise. The high accuracy attained by FFDNN IDS underscores its effectiveness in identifying anomalous behavior and enhancing network security within IoT contexts.

7. Recommendation

Our study concentrates on a limited number of IDS/ML models, allowing for a more comprehensive comparative analysis based on specific metrics such as accuracy, false positive rate, and computational complexity. We delve into the strengths and weaknesses of each model, discussing their real-world applicability and resilience against various types of attacks. Additionally, we integrate the results and findings of the Three-Way Selected Random Forest (3WSRF) model with those of existing IDS and ML approaches. This comparative analysis highlights the distinctive features, advantages, and potential drawbacks of the proposed model.

Acknowledging the limitations of the study, such as dataset biases and computational resources, and provide insights into future research directions. Consider exploring advanced feature selection techniques and evaluating the scalability of the 3WSRF model to larger network infrastructures.

8. Future Research Directions

The existing body of literature has furnished valuable insights concerning developing intrusion detection systems, emphasizing the utilization of random forest models in intrusion detection systems based on behavior. There arises a challenge in effectively choosing and classifying features and a decrease in the performance of classifiers during their construction. Furthermore, it is necessary to incorporate network traffic data for experimental analysis to ensure the proposed models' effectiveness for intrusion detection in practical scenarios. Future research endeavors should overcome these challenges by developing more advanced techniques for selecting features and combining ensemble learning algorithms with improved evaluation methods.

References

1. J. Ren, L. Liu, H. Huang, J. Ma, C. Zhang, L. Wang, B. Liu, Y. Zhao, "SOINN Intrusion Detection Model Based on Three-Way Attribute Reduction", Electronics 12, no. 24: 5023. 2023, https://doi.org/10.3390/electronics12245023.
2. M. Widianto, A. Sinaga, M. Ginting,(2022). "A Systematic Review of LPWAN and Short-Range Network using AI to Enhance Internet of Things". Journal of Robotics and Control (JRC), 3(4), 505-518, 2022, doi:https://doi.org/10.18196/jrc.v3i4.15419.
3. A. Alhowaide, I. Alsmadi, J. Tang, "Ensemble Detection Model for IoT IDS", Internet of Things, Volume 16, 2021, 100435, ISSN 2542- 6605, https://doi.org/10.1016/j.iot.2021.100435.
4. A. R. Abdulla, N. G. M. Jameel," A Review on IoT Intrusion Detection Systems Using Supervised Machine Learning: Techniques, Datasets, and Algorithms", UHD Journal of Science and Technology V(7), 1, 2023, DOI:10.21928/uhdjst.v7n1y2023.pp53-65.
5. S. Khonde, V. Ulagamuthalvi, "A Machine Learning Approach for Intrusion Detection using Ensemble Technique-A Survey", IJSRCSEIT, (3). 11:328-338, 2018.
6. I. priyadarsini, "Building an Efficient Intrusion Detection System Based on Feature Selection and Ensemble Classifier", Computer Networks, 2022, https://api.elsevier.com/PII:S1389128619314203.
7. N. Das, T. Sarkar, "Survey on host and network-based intrusion detection system", International Journal of Advanced Networking and Applications, vol. 6, no. 2, p. 2266, 2014.
8. L. Santos, C. Rabadao, R. Gonçalves. "Intrusion Detection Systems in Internet of Things: A Literature Review". In: 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, pp. 1-7, 2018.
9. Z. Chunying, W. Wang, L. Liu, J. Ren, L. Wang, "Three-Branch Random Forest Intrusion Detection Model", Mathematics 10, no. 23: 4460,2022, https://doi.org/10.3390/math10234460.
10. Hassan, M.; Butt, M.A.; Zaman, M. An Ensemble Random Forest Algorithm for Privacy Preserving Distributed Medical Data Mining. Int. J. E-Health Med. Commun. (IJEHMC) 2021, 12, 23.
11. Zong, F.; Zeng, M.; He, Z.; Yuan, Y. Bus-Car Mode Identification: Traffic Condition–Based Random-Forests Method. Journal of Transp.Eng. Part A Syst. 2020,146, 04020113.
12. Zhang, P.; Jin, Y.F.; Yin, Z.Y.; Yang, Y. Random Forest based artificial intelligent model for predicting failure envelopes ofcaisson foundations in sand. Appl. Ocean. Res. 2020, 101, 102223.

13. Z. Chunying , R. Jing, L. Fengchun, L. Xiaoqi, L. Shouyue, "Three way selection random forest algorithm based on decision boundary entropy", Applied Intelligence, 52. 1-14, 10.1007/s10489-021-03033- 7,2022,DOI:10.1007/s10489-021-03033-7.
14. Bhati, B.S.; Rai, C.S. Analysis of Support Vector Machine-based Intrusion Detection Techniques. Arab. J. Sci. Eng. 2020, 45, 2371– 2383.
15. Rajadurai, H.; Gandhi, U.D. Naive Bayes and deep learning model for wireless intrusion detection systems. Int. J. Eng. Syst. Model. Simul. 2021, 12, 111–119.
16. Hassan, E.; Saleh, M.; Ahmed, A. Network Intrusion Detection Approach using Machine Learning Based on Decision Tree Algorithm. J. Eng. Appl. Sci. 2020, 7, 1.
17. Xu, J.; Han, D.; Li, K.C.; Jiang, H. A K-means algorithm based on characteristics of density applied to network intrusion detection. Comput. Sci. Inf. Syst. 2020, 17, 665–687.
18. Liu, J.; Liu, P.; Pei, S.; Tian, C. Design and Implementation of Network Anomaly Detection System Based on Association Rules.Cyber Secur. Data Gov. 2020, 39, 14–22. https://doi.org/10.19358/j.issn.2096-5133.2020.11.003.
19. Jia, W.; Zhang, F.; Tong, B.; Wan, C. Application of Self-Organizing Mapping Neural Network in Intrusion Detection. Comput.Eng. Appl. 2009, 45, 115–117.
20. S. Zhang, Y. Li, "Intrusion Detection Method Based on Denoising Autoencoder and Three-way Decisions". Comput. Sci. 2021, 48, 345– 351.
21. J.Ranjith, K. Mahantesh, C. Abhilash, "LW-PWECC: Cryptographic Framework of Attack Detection and Secure Data Transmission in IoT". Journal of Robotics and Control (JRC), 5(1), 228-238, 2024 doi:https://doi.org/10.18196/jrc.v5i1.20514.
22. E. Hmouda, "A Validity-Based Approach for Feature Selection in Intrusion Detection Systems. Doctoral dissertation. Nova Southeastern University",NSUWorks, https://nsuworks.nova.edu/gscis_etd/1171,2022.
23. A. Paulo, D. André," A Survey of Random Forest Based Methods for Intrusion Detection Systems", ACM Computing Surveys. 51, 2018, doi:10.1145/3178582.
24. Saputra, D., Ma'arif, A., & Sunat, K. (2024). Optimizing Predictive Performance: Hyperparameter Tuning in Stacked Multi-Kernel Support Vector Machine Random Forest Models for Diabetes Identification. Journal of Robotics and Control (JRC), 4(6), 896-904. doi:https://doi.org/10.18196/jrc.v4i6.20898.
25. Bernard S, Heutte L, Adam S (2009) On the selection of decision trees in random forests. In: International joint conference on neural networks, IEEE, pp 302–307.
26. Meinshausen N (2010) Node harvest. Ann Appl Stat 4(4):2049–2072.
27. Oshiro T, Perez P, Baranauskas J (2012) How many trees in a random forest? Machine Learning and Data Mining in Pattern Recognition, pp 154–168
28. M. Kebede," K-Means Clustering and Random Forest Based Hybrid Intrusion Detection Algorithm", http://etd.aau.edu.et/bitstream/handle/123456789/12133/Meseret,201 9.
29. Ujjan, R.M.A.; Pervez, Z.; Dahal, K.; Khan, W.A.; Khattak, A.M.; Hayat, B. Entropy Based Features Distribution for Anti-DDoS Model in SDN. Sustainability 2021, 13, 1522
30. A. Bhattacharjee,"Cyber Security Intrusion Detection Deep Learning Model for Internet of Things", https://norma.ncirl.ie/5934/1/abhirupbhattacharjee.pdf ,2021.
31. E. Schultz, J. Mellander, and C. F. Endorf, "Intrusion Detection And Prevention McGraw-Hill Osborne Media," December, vol. 18, pp. 221-254, 2003.
32. A. D. Jadhav, V. Pellakuri, “Highly Accurate and Efficient Two Phase-Intrusion Detection System (TP-IDS) Using Distributed Processing of HADOOP and Machine Learning Techniques”, Journal of Big Data, 2021.
33. S. Mohammed, "A Machine Learning-Based Intrusion Detection of DDoS Attack on IoT Devices", International Journal of Advanced Trends in Computer Science and Engineering, 2021, 10, no. 4 (n.d.): 2792–97. doi:10.30534/IJATCSE/2021/221042021.
34. S. Pande, A. Khamparia, D. Gupta, D. N. H. Thanh. “DDOS Detection Using Machine

Learning Technique", Recent Studies on Computational Intelligence, 2020, 59–68. doi:10.1007/978-981-15- 8469-5_5.

35. S. A. Z. Mghames, A. A. Ibrahim, "Intrusion Detection System for Detecting Distributed Denial of Service Attacks Using Machine Learning Algorithms", Indonesian Journal of Electrical Engineering and Computer Science, 2023, Vol. 32, no. 1 (n.d.): 304. doi:10.11591/IJEECS.V32.I1.PP304-311.
36. [788] Ujjan, R.M.A.; Pervez, Z.; Dahal, K.; Khan, W.A.; Khattak, A.M.; Hayat, B. Entropy Based Features Distribution for Anti-DDoS Model in SDN. Sustainability 2021, 13, 1522.
37. Alam, T.M.; Awan, M.J. Domain analysis of information extraction techniques. Int. J. Multidiscip. Sci. Eng. 2018, 9, 1–9.
38. Koo, J.; Kang, G.; Kim, Y.-G. Security and Privacy in Big Data Life Cycle: A Survey and Open Challenges. Sustainability 2020, 12,10571.
39. A. Yang, C. Lu, G. Li, X. Huang, T. Ji, X. Li, Y. Sheng, Application of meta-learning in cyberspace security: a survey, vol 9 (1), pp 67-78, 2023, https://doi.org/10.1016/j.dcan.2022.03.007.
40. H. Hindy, E. Bayne, M. Bures, R. Atkinson, C.Tachtatzis, X.Bellekens, "Machine Learning Based IoT Intrusion Detection System", 12th International Networking Conference, vol 180, 2021, https://doi.org/10.1007/978-3-030-64758-2_6.
41. I. A. Abdulmajeed, I. M. Husien, "MLIDS22- IDS Design by Applying Hybrid CNN-LSTM Model on Mixed-Datasets", Slovene Society Informatika, Vol. 46,8, Pp. 121 – 134, 2022, Doi:10.31449/inf.v46i8.4348.
42. Khan, M.A.; Khan, M.A.; Jan, S.U.; Ahmad, J.; Jamal, S.S.; Shah, A.A.; Pitropakis, N.; Buchanan, W.J. A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT. Sensors 2021, 21, 7016. https://doi.org/10.3390/s21217016.
43. Mosaiyebzadeh, F.; Rodriguez, L.G.A.; Batista, D.M.; Hirata, R. A Network Intrusion Detection System using Deep Learning against MQTT Attacks in IoT. In Proceedings of the 2021 IEEE Latin- American Conference on Communications, Held, Santo Domingo, Dominican Republic, 17–19 November 2021; pp. 1–6. https://doi.org/10.1109/LATINCOM53176.2021.9647850 .
44. M. Al-Ambusaidi, Z. Yinjun,Y. Muhammad, "ML-IDS: an efficient ML-enabled intrusion detection system for securing IoT networks and applications", Soft Comput 28, 1765–1784 (2024), https://doi.org/10.1007/s00500-023-09452-7.
45. E. Altulaihan, M. A. Almaiah, Aljughaiman. "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms", Sensors 24, no. 2: 713, 2024, https://doi.org/10.3390/s24020713.
46. H. Alamgir, "Ensuring Network Security with a Robust Intrusion Detection System Using Ensemble-Based Machine Learning", ARRAY, 2023. doi:10.1016/j.array.2023.10030.
47. J. Mbugua, M. Thiga, J. Siror, "A Comparative Analysis of Standard and Ensemble Classifiers on Intrusion Detection System", International Journal of Computer Applications Technology and Research 8, no. 4 (2019): 107–15. doi:10.7753/IJCATR0804.1005.
48. S. R. Khonde, V. Ulagamuthalvi,"Hybrid Architecture for Distributed Intrusion Detection System Using Semi-supervised Classifiers in Ensemble Approach", Advances in Modeling and Analysis B, Vol. 63, No. 1-4, December, 2020, pp. 10-19, doi: 10.18280/ama b.631-403.
49. S. M. Kasongo, Y. Sun, "A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System", IEEE Access 7 (2019): 38597–607. doi:10.1109/ACCESS.2019.2905633.
50. K. K. kolli, "Predictive Model for Network Intrusion Detection System Using Deep Learning", Review Intelligence Artificial, 2020, doi: 10.18280/ria.340310.
51. I. Ahmad, Q. E. I. Ul Haq, M. O. M. Alassafi, R. A. AlGhamdi," An Efficient Network Intrusion Detection and Classification System", Mathematics, 2022, 10, 530 ,

https://doi.org/10.3390/math10030530.

52. A. F. Mukeri, D. P. Gaikwad, "Adversarial Machine Learning Attacks and Defenses in Network Intrusion Detection Systems", International journal of wireless and microwave technologies,8 (10),2022, DOI: 10.5815/ijwmt.2022.01.02.
53. M. H. Shahzad, H. M. Ali, "Adversarial Training Against Adversarial Attacks for Machine Learning-Based Intrusion Detection Systems", Computers Materials Continua, 2022,Vol. 73, no. 2 (n.d.): 3513–27. doi:10.32604/CMC.2022.029858.
54. P. Papadopoulos, O. Thornewill, N. Pitropakis, C. Chrysoulas, A. Mylonas, W. J. Buchanan. 2021. "Launching Adversarial Attacks against Network Intrusion Detection Systems for IoT", Journal of Cyber security and Privacy, Vol. 1, no. 2: 252-273. https://doi.org/10.3390/jcp1020014.
55. B. S. Khater, A. W. Abdul Wahab, M. Y. I. Idris, M. A. Hussain, A. A. Ibrahim, M. A. Amin, H. A. Shehadeh," Classifier Performance Evaluation for Lightweight IDS Using Fog Computing in IoT Security", Electronics, 2021, doi.org/10.3390/electronics.10141633.
56. A. A. Yilmaz, "Intrusion Detection in Computer Networks Using Improved Machine Learning Algorithms," 3rd International Informatics and Software Engineering Conference, 2022, DOI: 10.1109/IISEC56263.2022.9998258.
57. A. Kaveh, A. Pettersson, C. Rohner and A. Johnsson, "On the Impact of Blackhole-Attack Variations on ML-based Intrusion Detection Systems in IoT," NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, 2023, pp. 1-4, doi: 10.1109/NOMS56928.2023.10154213.
58. N. Tekin, A. Acar, A. Aris, A. S. Uluagac, V. C. Gungor,"Energy consumption of on-device machine learning models for IoT intrusion detection", Internet of Things, Vol 21, 2023, doi.org/10.1016/j.iot.2022.100670.
59. I.A. Abdulmajeed, I. M. Husien, "Machine Learning Algorithms and Datasets for Modern IDS Design", 6th IEEE International Conference on Cybernetics and Computational Intelligence, CyberneticsCom 2022, pp. 335 – 340, doi:10.1109/CyberneticsCom55287.2022.9865255.
60. T. S. Yange, O. Onyekware, Y. M. Abdulmumin,"AData Analytics System for Network Intrusion Detection Using Decision Tree", JCSA, Vol. 8, no. 1, 2020, pp(21-29), doi: 10.12691/jcsa-8-1-4.
61. Y. Shen," An Intrusion Detection Algorithm for DDoS Attacks Based on DBN and Three-way Decisions", J. Phys.: Conf. Ser. 2356. 012044, 2022, DOI :10.1088/1742-6596/2356/1/012044.
62. M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, H. Janicke, "RDTIDS: Rules and Decision Tree-Based Intrusion Detection System for Internet-of-Things Networks", Future Internet 12, no. 3 (2020): 44. doi:10.3390/FI12030044.
63. I. Publication, "EXPERIMENTAL ANALYSIS OF DECISION TREE CLASSIFIER IN INTRUSION DETECTION", IAEME PUBLICATION, 2020, doi:10.34218/IJARET.11.7.2020.085.
64. R. Chowdhury, P. Banerjee, S. D. Dey, B. Saha, "A Decision Tree Based Intrusion Detection System for Identification of Malicious Web Attacks", Preprints 2020, 2020070191. https://doi.org/10.20944/preprints202007.0191.v1.
65. S. M. Mousavi, V. Majidnezhad, A. Naghipour, "A New Intelligent Intrusion Detector Based on Ensemble of Decision Trees", Journal of Ambient Intelligence and Humanized Computing 13, no. 7 (2019): 3347–59. doi:10.1007/S12652-019-01596-5.
66. I. Sarker, "IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model." Journal: Symmetry (SCI), 2020,12,754,doi:10.3390/sym12050754.
67. S. Wasir, P. Dubey, "A DECISION TREE BASED TECHNIQUE FOR CLASSIFICATION OF IDS DATA SET." International Journal of Engineering Sciences Research Technology 9, no. 6 (2020): 55– 60. doi:10.29121/IJESRT.V9.I6.2020.10.

68. L. A. C. Ahakonye, C. I. Nwakanma, J. Lee, D. Kim ,"SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection Internet of Things",Vol. 21, https://doi.org/10.1016/j.iot.2022.100676.
69. Y. J. Chew, S. Y. Ooi, K. S. Wong, Y. H. Pang, N. Lee, "Adoption of IP Truncation in a Privacy-Based Decision Tree Pruning Design: A Case Study in Network Intrusion Detection System" , Electronics 11, no. 5: 805, 2022, https://doi.org/10.3390/electronics11050805.
70. Y. Lan, T. Truong-Huu, J. Wu and S. G. Teo, "Cascaded Multi-Class Network Intrusion Detection With Decision Tree and Self-attentive Model," 2022 IEEE International Conference on Data Mining Workshops (ICDMW), Orlando, FL, USA, 2022, pp. 1-7, doi: 10.1109/ICDMW58026.2022.00081.
71. R. TEKIN, O. YAMAN, T. TUNCER, "Decision Tree Based Intrusion Detection Method in the Internet of Things", IJIEA, Vol. 6, no. 1, pp. 17-23, 2022, doi: 10.46460/ijiea.970383.
72. B.S. Amrutha, I. Meghana, R. Tejas, H.V. Pilare, D. Annapurna, "An Efficient Automated Intrusion Detection System Using Hybrid Decision Tree", Inventive Systems and Control, vol 436. (2022), doi.org/10.1007/978-981-19-1012-8_49.
73. J. Mehta, G. Richard, L. Lugosch, D. Ya, B. H. Meyer, "DT-DS: CAN Intrusion Detection with Decision Tree Ensembles", ACM Transactions on Cyber-Physical Systems, Vol. 7(1), pp 1–27, https://doi.org/10.1145/3566132.
74. B. K. Nirupama and M. Niranjanamurthy, "Network Intrusion Detection using Decision Tree and Random Forest," International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-9, doi: 10.1109/ACCAI53970.2022.9752578.
75. D. Santhadevi, B. Janet, "EIDIMA: Edge-based Intrusion Detection of IoT Malware Attacks using Decision Tree-based Boosting Algorithms", Lecture Notes in Electrical Engineering, 2022,vol 853, https://doi.org/10.1007/978-981-16-9885-9_37.
76. T. Le, H. Kim, H. Kang, H. Kim, "Classification and Explanation for Intrusion Detection System Based on Ensemble Trees and SHAP Method", Sensors 22, no. 3: 1154, 2022, https://doi.org/10.3390/s22031154.
77. A. R. Zarzoor, N. A. S. Al-Jamaliy, "Intrusion detection method for internet of things based on the spiking neural network and decision tree method", Vol. 13, No. 2, April 2023, pp. 2278~2288 ISSN: 2088- 8708, DOI: 10.11591/ijece.v13i2.pp2278-2288.
78. A. Al-Saleh, "A balanced communication-avoiding support vector machine decision tree method for smart intrusion detection systems". Sci Rep 13, 9083 (2023), https://doi.org/10.1038/s41598- 023-36304-z.
79. B. Mahbooba, M. Timilsina, R. Sahal, M. Serrano, “Explainable Artificial Intelligence (XAI) to Enhance Trust Management in Intrusion Detection Systems Using Decision Tree Model”, Complexity 2021, 1–11, doi:10.1155/2021/6634811.
80. Cannings TI, Samworth RJ (2017) Random-projection ensemble classification. J R Stat Soc Ser B (StatMethodol) 79(4):959–1035