American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-13, Issue-3, pp-92-111
www.ajer.org
Research Paper Open Access

Entropy-based Detection of DOS Attacks in IoT devices using Multi-Classifiers

M Mattah Islam Sameem
Dept. of Computer Science
National University of Computer and Emerging Science
Islamabad, Pakistan

Qaisar Shafi
Dept. of Computer Science
National University of Computer and Emerging Science
Islamabad, Pakistan

Adnan Fazil
Dept. of Avionics Engineering
Air University
Islamabad, Pakistan

Khush Bakhat Awar
Faculty of Computing and AI
Air University
Islamabad, Pakistan

M Shujah Islam
Dept. of Computer Science
King Faisal University
Al-Ahsa 31982, Saudi Arabia

Abstract—*DOS attacks indicate a substantial risk to the security and stability of Internet of Things (IoT) devices. The risk of such attacks is increasing due to the growth of IoT devices and their interconnection. Unfortunately, current approaches for detecting DOS assaults on IoT devices have some drawbacks and are sometimes ineffective, leaving IoT networks vulnerable to potentially disastrous effects. The problem of creating a more reliable mechanism for identifying DOS attacks on IoT devices is discussed in this study. Our study suggests a multiclassifier system that uses a voting-based methodology to distinguish between legitimate traffic and denial-of-service (DOS) attacks on Internet of Things (IoT) devices. This solution solves the security issues posed by IoT devices by utilizing machine-learning approaches to increase classification accuracy. We specifically look into the usage of entropy-based features using a multiclassifier system that combines the Support Vector Machine (SVM), Alternating Decision Tree (ADT), and Multilayer Perceptron (MLP) classifiers. This method is used with the CIC IoT Dataset 2022, the most recent IoT-based dataset. The dataset's features are extracted using an entropy-based method. In particular, Shannon entropy is used to gauge how unpredictable the dataset is. Our findings demonstrate that, for home-based IoT devices and security cameras, our multiclassifier model beats the single classifier technique with true positive rates (TPR) of 99.1% and 99.2% percent. Through K-fold cross-validation with 2, 4, 6, 8, and 10 folds, we further assess the performance of our model. Our research suggests that a promising strategy for identifying DOS assaults on IoT devices is the entropy-based detection method using multiclassifiers. However, when evaluating the findings, it is essential to consider the dataset's constraints and inherent biases.*

Keywords—*IoT; DOS; Multiclassifier; Deep learning; Machine learning*

Date of Submission: 15-03-2024 Date of acceptance: 31-03-2024

I. INTRODUCTION

The Internet of Things (IoT) network is evolving and increasing rapidly; these devices are connected to the Internet, which means cybercriminals have a chance to attack vulnerable IoT devices [1]. DOS attacks are dangerous, and detection becomes challenging as new devices come to market [2]. The risk of distributed denial of service (DOS) attacks is always there for online devices [3]. These intelligent IoT devices can perform exceptionally well in the lives of humans; therefore, it is necessary to focus on their security. Over the last few years, DOS attacks have been increasing. Denial of service is an attack in which a massive amount of traffic is reaching the same destination (Victim) by some sources (attacker) by which the limit is overwhelmed [4]. The services (destination) stop working. The attacker keeps sending too much data continuously until denial of service occurs, in which services halt. The user cannot access the application or any service, and the attacker can take some benefits in this scenario. To stop or slow down service, a denial-of-service (DOS) assault might be launched. The Internet of Things (IoT) is the largest and most easily accessible network to which any smart device may connect, and its security is paramount. The denial-of-service (DOS) assault is the most dangerous attack that has emerged throughout the IoT. The Internet of Things (IoT) is a technological advancement that has made our lives much more convenient by linking various appliances, such as computers, phones, and even things like fridges and dishwashers, together in one system. Many security and privacy issues have emerged due to the proliferation of IoT devices, significantly hampering the ability to gather, analyse, and correlate data centered on IoT. IoT systems present substantial challenges in identifying security vulnerabilities and assaults due to the rapid rise of threats and various attacks. With the growth in the number of IoT devices, the amount of traffic created by IoT-based attacks has rapidly grown. IoT DOS attacks, which aim to perform accurate, efficient, and effective cybercrimes, are one of the most concerning threats associated with the IoT. Most IoT devices are vulnerable because they use the default password [5]. In a DOS attack, legitimate users will suffer slow or no access to the device or services. The attackers use the latest techniques and do not care for minor or vast companies, whether non-profit or big-profit organizations, which can become victims of these cybercriminals. These organizations' devices can be slowed or completely halted by a denial of service (DOS). There is also a lack of knowledge about cyber threats among people, employees, and organizations, as they can become victims just because of a lack of knowledge. Most organizations run nonstop to provide their services to clients, which must be secured and uninterrupted. There are also critical infrastructures and financial pillars of a country, such as banks or affiliated organizations such as microfinance banks, currency exchanges, and stock exchanges. They are so vital that their continued operation is required to guarantee a given country's security and the country's economy, people's health, and safety. In the modern era of the cyber defence system, the approaches used by cybersecurity experts to protect devices by using machine learning techniques by monitoring the traffic patterns of the devices. They [6], showed the machine learning techniques for IoT devices for the Internet of Things (IoT). Conventional IDS frameworks are not developed to work effectively in an IoT network as these gadgets have limited memory and scanty functionality. Multiple methods exist for defending against DOS attacks, including signature-based detection. Unlike Entropy-based features, detection systems are effective against freshly emerging attack patterns. DOS attacks may evade conventional channels and intrusion detection systems. IoT devices differ from conventional ones because they use communication protocols that guarantee precise data exchange. They are more vulnerable to attacks as a result. We present a multiclassifier system. This system uses machine learning techniques to improve accuracy. We can discern between DOS attacks and legitimate traffic using our voting-based system. In particular, the Support Vector Machine (SVM), Alternating Decision Tree (ADT), and Multilayer Perceptron (MLP) classifiers are combined into a multiclassifier system. The most recent IoT-based dataset, the CIC IoT Dataset 2022, is used with this technique. Entropy-based techniques are used to extract the features of the dataset. Using entropy-based feature extraction with Shannon entropy, we improve detection and classification accuracy to address IoT security challenges.

A. Motivation

There has been a quick surge in IoT device numbers. Manufacturers of these devices intend to produce the maximum number of IoT devices. They have placed considerably less priority on IoT device security. According to [13], the resource-constrained nature of IoT devices makes them an accessible target for attackers. Most researchers use a single algorithm to classify DDOS attacks. We will use three classifiers to learn more about this domain and how multiple classifiers can react to the latest IoT dataset. There is no simple way to guarantee the safety of all Internet of Things (IoT) systems due to the diversity of these services and applications [14]. Multi Classification System strategies for protecting against denial-of-service attacks are covered here.

Due to the IoT's potential uses across a wide range of fields, several research contributions have recently been noted in this field. With the help of different technologies, IoT offers a viable answer to make life easier and more enjoyable for customers. IoT technologies have also become more well-known thanks to the growth of big data and remote storage applications. New IoT applications have surfaced because of readily available resources. Smart homes, wearable technologies like fitness bands, linked autos, industrial internet, smart cities, IoT in agriculture, IoT in healthcare, smart retail, and energy engagement are a few examples of popular new IoT applications [21]. Due to the rapidly developing apps and linked devices, security is now more important than ever. Additionally, the utilization of the data gathered from IoT devices raises questions about how and where this data may be utilized. This is one of the driving forces for our investigation. The key contribution of our study ultimately comes from our realization that a comprehensive examination of machine learning (ML) and deep learning (DL) for protecting IoT networks against intrusions has to be conducted.

For DDOS attack detection, there are numerous solutions like signature-based and anomaly-based detection systems. We will use an anomaly-based detection system to deal with unknown threats. Anomaly-based detection can help us identify new attacks. For better training, a better dataset is required, but the latest datasets are complex and have many features, so we will research our approach using the latest IOT-based datasets. Over time, attackers discover new vulnerabilities; as a result, their attack vectors, techniques, and approaches differ from those of previous attacks, as they can protect devices from future attacks through reactive measures. Modern datasets are complex and versatile, so exploring them requires deep learning techniques. In the future, DDOS attacks will become so prevalent that Cisco predicts the number of attacks will double, from 7.9 million in 2018 to over 15 million in 2023 [15]. As the development of IoT security is currently in its early stages, attackers' techniques are evolving, and their attacks are mutating. We observe new attacks on Internet of Things (IoT) devices, making it difficult for cyber experts to test the model using previous datasets. Using additional, rich features in the feature extraction phase will improve the accuracy and other evaluation parameters. Monitoring malicious activities through machine learning techniques is beneficial.

B. IoT

IoT devices are the kind of products linked to the internet, and they are physical objects. There are several types of IoT devices available in the market. IoT devices are different from our traditional devices, and communication and connection are different from other devices. Knowing these devices are resource-constrained, connected by a gateway or built-in functionality. The Internet of Things is the internet of networks. The Internet of Things, or IoT, refers to the network formed by the networked connectivity of everyday objects with embedded computer technology, such as mobile phones, handsets, routers, and dishwashers. It paves the way for all those objects [2] and more to communicate and share information, including a wide range of sensor-equipped everyday items. Water, traffic, temperature, energy, and sensors are all excellent examples. The Internet of Things must be conceived of as a service. Accessing everything anytime is made possible by centralizing everything (our gadgets and data) in a single location (data centers). The data will be examined based on our requirements, and the instructed action will be taken. Modern automobiles, for instance, have a variety of control systems for the engine, safety features, and communication networks. Commercial and residential buildings use different heating, ventilation, air conditioning (HVAC) systems, phone services, security measures, and lighting systems. As the Internet of Things develops, these technologies will be linked to enhanced security, analytical, and management features. Due to this, IoT will be able to help people more effectively than ever before. Internet Of Things IoT devices utilize IoT protocols for communication, and protocols differ from traditional ones. Attackers' approaches and mindsets are also different compared to traditional devices. IoT devices are the driving force behind current Distributed Denial-of-Service (DDOS) attacks because they are used to build a botnet, a network controlled by a hacker. By controlling these IoT devices, hackers may execute Distributed Denial-of-Service (DDOS) attacks on any website. Hackers exploit vulnerabilities. Users and manufacturers are unaware. Users who do not add a password, use the manufacturer's default password, and are uninformed of upgrades may become victims. Some need to pay attention to regular updates. Companies are more interested in producing IoT devices than securing them, shipping them worldwide, and selling them to users.

C. Possible attacks on IoT

Here, we took a quick look at the framework of the Internet of Things. TCP/IP, a four-layer model, has replaced the older OSI model, a seven-layer model, as the foundation for modern networking design. The terms" application," transport," network," and" network interface" refer to these levels. The OSI and TCP/IP models' layer-based protocols and services are IoT technology that uses the very same framework [8]. The IoT's layered networking architecture consists of the Application Layer, Perception Layer, Network Layer, and Physical Layer. As shown in Figure, each of these levels makes possible a unique set of technological possibilities. A layer of Applications: IoT's application layer features a wide range of useful services, such as"

Smart Cities,”” Smart Transportation,” and so on. The layer of Perception — This layer offers sensory technology like Sensor Nodes, RFID Sensors, etc. This layer is responsible for facilitating communication between nodes in the network. In this area, information is exchanged between various gadgets. The Internet of Things (IoT) is realized by the physical components of the Physical Layer. Health care, environmental monitoring, home automation, smart transportation, and Industry 4.0 are just a few of the areas where the Internet of Things (IoT) is rapidly expanding. The proliferation of IoT devices in homes and businesses is making them the norm. Data leakage, denial-of-service attacks, unauthorized access to networks, etc. are all potential outcomes without adequate cybersecurity measures in place. Inadequate security measures are present in many low-end commercial IoT products, making them vulnerable to exploitation in security attacks. Threats to these tiers’ security or malicious activity might disrupt service delivery. Furthermore, undesirable and perhaps harmful outcomes might result from services not functioning properly. the dangers that might penetrate these levels. It would be challenging to provide fixes for software issues due to the diverse nature of the IoT. The application layer will suffer as a result of this. Malware like ransomware may flourish in such an atmosphere. Sniffing and eavesdropping are two examples of assaults that may target the perception layer. Disruption of service attacks (DOS) is a prevalent danger to the network layer. When it comes to the physical layer, power outages, and hardware failures are the biggest threats to security. Despite this organization, faults in these levels affect the safety of the whole system. When it comes to IoT devices, denial-of-service attacks are a major concern because of resource limitations. Therefore, the goal of a denial-of-service attack is to prevent people from accessing a computer or network resource (clients, senders, etc.). When an attacker floods the primary server or host with requests, denial of service (DOS) happens on the Internet of Things. To prevent legitimate requests and traffic from accessing the network, the attacker node is utilized to flood either traffic or requests. Indirectly, the rogue node stops other nodes from connecting to the server. The attacking node will attempt to cut off communication with all other nodes. As a result, the attacked node will function poorly.

D. DDOS attack

DDOS attacks are organized, large-scale assaults on the service availability of a target system or network resource that are initiated remotely from several infected computers throughout the Internet. The” main victim” is the organization whose services are being disrupted, while the” secondary victims” are the compromised systems being utilized to launch the assault. Using secondary victims in a distributed denial of service (DDOS) assault allows the attacker to launch a more extensive and disruptive attack, difficult to identify and block the initial attacker connections using genuine (non-malicious) clients.

Due to the limitations of existing network components, the variety of attack techniques, and the operators’ opacity to host sites, DDOS assaults are among the most difficult security issues to identify, fight against, and track. Although there are active defences against DDOS assaults, such as firewalls and vendor-specific updates, they are not fully effective. Recent tests using the SYN attack, one of the most well-known DDOS assaults on commercial platforms, have shown that a server may be overwhelmed with only 500 SYN packets per second of attack traffic.

E. DOS Attack

In a denial-of-service attack, the attackers make an effort to stop legitimate users from accessing the service. The assault primarily focuses on obtaining access to otherwise unprotected resources including processing time, memory, and storage space. Overloading the server with requests is a common tactic in this kind of attack. As a result, the server becomes less responsive to queries and may eventually cease responding altogether. The UDP flood, ICMP flood, SYN flood, HTTP flood, etc., are only a few of the most popular types of assaults. In our work, we have applied our technique by using Flood attacks. In a Syn Flood attack, the attacker takes advantage of the TCP three-way handshake communication to exploit it causing congestion in a network. Figure 1 depicts the typical TCP three-way handshake communication. We have observed different communication in IoT devices because the nature of IoT devices is different from each other. Here are steps by which a normal three-way handshake occurs in an IoT device

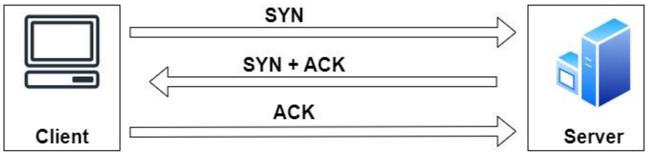


Fig. 1. Three-way Handshake

- client initiates communication with the server by sending a SYN message.
- the server sends a synchronize-acknowledge (SYN-ACK) message to the client.
- the client responds to the server with an acknowledgment (ACK) message.

An SYN flood attack involves the continuous transmission of SYN packets to any and all listening ports on the victim server. The server will send SYN-ACK packets in response and wait for the attackers) ACK message from the client. However, the attacker does not respond with an ACK, therefore the server remains connected. After a certain point, the server's connection table will be at capacity, and it will no longer be able to support legitimate users. In this work, Flood attacks are performed by using a low-orbit ion cannon tool.

F. Entropy

A statistical metric called entropy depicts the unpredictability of a collection of data. The field values of the packets that were received in our situation are the data set. Since an attacker continuously delivers identical packets, packet attributes gradually become less random. However, entropy measurement is a useful tool for monitoring these unforeseen variations in randomness. Every sort of attack alters the randomness of various IP packet parameters, such as the destination port. We use the most impacted IP packet fields to calculate entropy. Entropy, or randomness, may be measured simultaneously for many IP packet fields. We may use entropy calculation to identify various assault types utilizing this property. This approach works even if there are fewer malicious packets than genuine packets since the randomness will abruptly change when the intensity of the examined attribute data increases at certain locations.

Entropy-based statistical methods provide significant benefits for DOS assault detection. This method simply looks at arriving packets; thus it doesn't increase the amount of network traffic. The overhead for memory and the CPU is also quite little. We use Shannon entropy for this investigation [ref]. According to the literature, Shannon entropy that has been modified for DDOS detection is;

$$\text{H}= \sum_{n=0}^{M-1} P(x_n) log(P(x_n)) \qquad (1)$$

In this case, P stands for the probability that the event X will occur, where X is the attribute value and M is the total number of possible attribute values. Here," attribute" refers to the fields examined in network packets.

Machine learning is indeed only feasible with the availability of data, and with excellent relevant data, we were able to train our model with the aid of machine learning. Machine learning can help us solve cybersecurity issues. A smart system will learn and then forecast. We will adapt our approach to learning and evolving which is a self-learning system. Entropy is used in machine learning to evaluate the degree of disorder in processing information. Entropy is often employed in modern DOS attack detection systems to provide beneficial traffic categorization properties. Entropy is a statistical measure of information uncertainty. Entropy is a single-valued statistic that reflects network traffic dispersion.

Knowledge theory based on entropy is utilized to establish a link between class property and other characteristics. To quantify the dispersion of a random variable, statisticians use a quantity called entropy. Obtaining entropy may be done with the help of the following formula. If plug in some numbers, we get:

$$H(X) = P(x_n) log(P(x_n)) \qquad (2)$$

Furthermore, the equation describes the entropy of the attribute X (class) after considering the values of another element Y. The formula for the ratio of X to Y is:

$$H(X/Y) = \log_2(P(x_i/y_j)) \qquad (3)$$

where $P(x_i/y_j)$ is the reciprocal of the X-Y ratio. For all possible values of X, $P(x_i)$ represents the prior probability, whereas $P(x_i/y_j)$ represents the posterior probabilities given values of Y. Knowledge gain or the amount by which X's entropy lowers as a result of Y's contribution of new information about X (a class property), is calculated as follows:

G. Multiple Classifier System(MCS)

Combining several machine learning classifiers to create a broader and more accurate classification system is known as a Multiple Classifier System (MCS). Our MCS technique relies on entropy-based characteristics to recognize a specific sort of DOS assault. Some previous efforts had less entropy-based features. We suggest a detection method that uses the latest datasets and MCS-based classifiers for identifying various DOS attacks accurately. By using MCS, the efficiency of the system will increase instead of a single classifier. MCS is a voting-based system in which two classifiers will run for a majority and a third classifier will act as a judge. Our voting-based system 2 uses entropy-based characteristics to identify DOS attacks and differentiate between malicious and everyday activities.

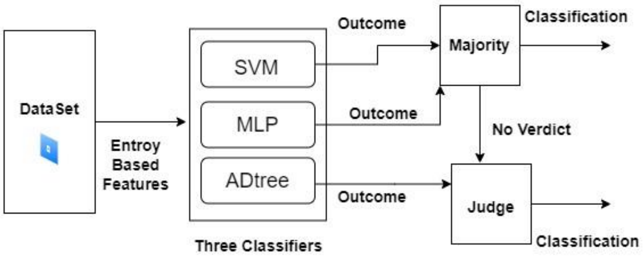


Fig. 2. Multi-Classifier system

II. INTRUSION DETECTION SYSTEMS FOR IOT

A direct result of advancements in areas like sensors, automatic item identification and tracking, device-to-device communication, and integrated and distributed Internet services is a greater reliance on smart gadgets. The increased risks for Internet services and equipment, however, are a direct result of the rising demand for IoT devices with useful applications [1]. For instance, false alarms in home appliances that jeopardise privacy and personal security as well as breakdowns in electricity and transportation systems that disrupt daily life in cities and countries are security concerns to CPSs based on critical infrastructure. As a result of exposure to the weaknesses in system resources, the security requirements of both the user and the system are in jeopardy. The Nest smoke alarm, Belkin WeMo power switch, and Phillips Hue light bulb were utilized as demonstration smart home appliances in [4]. Studies showed that security and privacy can be easily exploited due to the network's connected devices' low power and processing capabilities. It takes a lot of work to provide reliable security solutions for IoT networks so that users may take advantage of the possibilities that IoT devices offer while still adhering to security regulations [5].

When a breach is discovered, an IDS is able to monitor the network activity between the linked devices and create an alert [6]. Due to its capacity to monitor and alarm, an IDS is regarded as a crucial protection measure for conventional IP networks. Even though IDS works well for conventional networks, creating IDS for an IoT network is a difficult undertaking. This is due to IoT network features including the network's IDS agent nodes' constrained processing and storage capacities [7]. While IoT network nodes are digitally augmented with sensors, actuators, programming logic, and communication interfaces, conventional IP networks assign IDS agents with the capacity to function in constantly changing environments. IoT networks have a problem in developing nodes with these characteristics and ensuring security. Typically, nodes in IP networks have dependable connections and forward packets from source to destination. IoT networks, however, may not necessarily have linked devices. The gadgets have sporadic connections and will connect every so often in order to save bandwidth and energy. For instance, sensor nodes in IoT-based home alarm systems might communicate across small distances and have sporadic connections [4].

TABLE I SURVEY TABLE

Publisher	*Year*	*Strategy*	*Main Contributions*
ACM [17]	2007	Survey	Analyse the design decisions
ACM [32]	2019	Extensive Review	utilizes its abilities to secure conventional networks
ACM [33]	2006	Implementation, Analysis	Experiment under various conditions
IEEE [34]	2016	Information Flow Analysis	Examines active detection mechanisms
IEEE [35]	2017	Implementation	Introduce the notion of "sparse strong observability" to characterize systems
IEEE [36]	2013	Model Base Techniques	Problem formulation was analyzed and countermeasures
Springer [37]	2011	Analysis	Execution of IBL model generates predictions

III. LITERATURE REVIEW

As discussed by [15]. The number of IoT devices will be around 100 billion in this IoT ecosystem by 2025, all connected to the internet. IoT devices are helping people to socialize, save time, or entertain themselves with all these benefits. There are also some disadvantages to these devices. If applicable, we must take care and take action to generate the maximum benefit from these IoT devices. There is a need for security and uninterrupted operation of these systems and devices for these online services. According to [16], these devices are connected to an open network. That is why these IoT devices are so vulnerable. IoT devices are valuable devices and must require attention to their security because users have less technical knowledge and mostly do not do anything for security measurements. Information security is essential nowadays; after making these types of devices that share data through the internet must need information security. It's like doing it to avoid unauthorized access. Information security has a core pillar: information must always be available when there is no temper or break. Cybersecurity is used for protecting mobile phones, computers, servers, network routers, constrained resources, Internet of Things (IoT) devices, etc., from malicious attacks. According to [17], attackers quickly attack IoT devices because of their resource-constrained nature. In this paper, they discussed that attackers could attack IoT devices. In this research paper, Cisco predicted DDOS attacks would double from 2018 to 2023, So there is much space to research DDOS protection from IoT devices.

In [18] The research on IoT devices attacks only focuses on the Mirai attack and its modified versions. The authors state that they only proposed detection and mitigation in Lebanon and did not extend their work to other countries. Most Internet of Things (IoT) devices are susceptible to cyberattacks and can quickly become victims, putting the entire organization at risk. [3]. Proposal [19] In their study, they have created and suggested the concept of real-time machine learning approaches to identify and mitigate DOS attacks on IoT devices. However, they have not yet applied these techniques in a Cloud context. In [20]. They highlighted how botnets spread the DDOS assault across the internet globe. They offer a solution based on honeypots. This article is also significant to our study since its methodology is consistent with zero-day attack detection. They have suggested and executed the idea of honeypots. However, they only offer cloud-based real-time detection. In [20] They offer a new technique based on a honeypot named IoTCMal". They addressed malware accessible from eleven groups of attackers. They examined eleven malwares on IoTCMal and compared them. This study presents several forms of malware and their behaviors. We may use algorithms based on machine learning to identify and mitigate DDOS assaults.

TABLE II COMPARISON TABLE

Publisher and Year	*Approach*	*Dataset*	*Evaluation Metrics*	*Limitations*
TNSM [13] (IEEE) 2022	Proposed a lightweight DL model named LUCID	ISCX2012 CIC2017	FPR, TPR F1-score, Accuracy	Comparative aspects for features needs explanation.
MDPI [27] 2021	DDOS detection using anomaly ESPRT	DARPA 1999 DARPA 2000 CIC-DDOS2019	Accuracy F1-Score TPR, FPR	Ignored low intensity attacks
MDPI [26] 2020	CNN based IDS for binary	multiclass classification	CSE-CIC-IDS 2018, KDD Precision, F1-score	Low accuracy for RNN
IEEE [5] 2020	DDOS countermeasure architecture	NIL	NIL	No discussion on DDOS types
IEEE [29] 2020	Flow Guard protection for IOT devices	CICDDOS2019	Accuracy, F1-score	Computationally expensive
IEEE [28] 2018	approach to deal with vulnerability in CLDAP	NIL	Bandwidth	Less bandwidth packets not considered
IEEE [25] 2018	SDN using anomaly based architecture	UNSW-NB15	F1-score ROC curve Accuracy	Performance is comparably unstable using RNN and MLP
ICOIN [10] (IEEE) 2018	Entropy Based Multiclassification System	ISCX 2012	Accuracy F-1 score	Dataset limited features
IEEE [19] 2017	Honey pot simulation	NIL	Efficiency percentage	Accuracy decreases with increase in Bots
ICACCA [30] 2016	Multiclassifier System	NSL-KDD99	Accuracy, ROC Curve	OLD Dataset
IEEE [31] 2015	Comparison of ML models for DDOS	DARPA2000 CAIDA2007	Accuracy FN,FP rate	OLD and limited dataset

In [21]. A novel methodology is presented. Researchers have implemented a semi-supervised technique in their novel model for detecting and mitigating DDOS attacks in IoT. Researchers have proposed numerous machine learning detection systems for IoT devices. the solution proposed by [15] In a study using IoT devices, researchers presented a machine learning-based real-time approach for malware classification. [3]. IoT devices are now in human culture since users can connect to the internet and remotely control IoT devices. [15] The number of IoT devices will be around 100 billion in this IoT ecosystem by 2025, and all are connected to the internet. In upcoming years, DDOS attacks will be so common that the number of attacks will double, as predicted by Cisco (i.e.) from 7.9 million in 2018 to almost 15 million in 2023. Protecting devices from cybercriminals is a big issue. [5]. Big organizations like Cisco and Linksys have been affected by the DDOS attack [23]. IoT devices are limited in computing, storage, and network capability, making them vulnerable to exploitation. [3] When these devices are directly connected to the internet, malicious actors can detect and attack them. Due to limited resources, defending the IoT system from malicious attacks is challenging. [3] One of the common challenge attacks on IoT is the Hijacked Devices Conscripted into the Botnets attack [24]. Hackers will launch denial-of-service (DDOS) attacks against the target host via infected IoT devices controlled by a command and control server. Zero-day DDOS Attacks have emerged as an open challenge in defending IoT against DDOS Attacks [5]. We face the latest DDOS attacks because attackers are using the latest techniques.

In [25] SDN-aided detection for IoT networks uses fog to identify several attack models in near real-time for effective threat mitigation. Also, new technologies are increasing the usage of detection. SDN-aided detection for IoT networks employs fog to identify attack models in real time. In [13] Classification performance, source/destination identification, memory consumption, and computation cost are only a few of the aspects impacting DDOS attack detection techniques' effectiveness. A statistical attack detection system's accuracy and speed are the most crucial variables to consider, particularly if the anomaly detection acts on behalf of a user. In [26] DOS category in several datasets is the subject of this study, and a DL model for DOS identification is developed. We use a Convolutional Neural Network (CNN) to build our model and compare its results to a Recurrent Neural Network (RNN). Furthermore, we recommend the best CNN design based on extensive experimentation.

Machine learning (ML) and deep neural networks (DNN) models to identify and defend against DDOS attacks in Software Defined Networks (SDN) [13]. It is possible to reduce the negative impact of DDOS on a system by using a mix of machine learning and deep machine learning. One of the two kinds of attacks we tested was a cyberattack performed by a security expert.

ESPRT [27] identifies DDOS assaults which include entropy with multiple datasets utilized to examine the implementations. In [19] They gather and examine the outcomes of the developed method once it has been applied in a real-time setting using some different embedded systems that are linked by a virtual system. In [28] They suggest a strategy to limit the amount of information that CLDAP generates in amplified attacks, which utilizes the DDOS threat efficient security system. Flow Guard [29]: An Intelligent Edge Defence Mechanism Against IoT DDOS Attacks Develop and implement two ML models for

DDOS detection and categorization algorithms using artificial intelligence. Counteraction against Internet of Things Botnets in Private Networks Devices may encourage the creation of IoT botnet countermeasures in private networks and global norms for IoT security discussed [5]. The above TABLE I shows a comparison of different research papers where the survey is done. The comparison of the approaches in the research papers related to my area of interest is shown in Tables II & III.

IV. METHODOLOGY

A. Proposed Approach

We proposed an approach for IoT devices not to become victims of DOS attacks, as they are vulnerable because of their resource-constrained nature. As discussed earlier, there is a rise in DOS attacks that involve IoT devices. Since IoT devices are well-known victims of DOS attacks, it is crucial to identify attacks that separate malicious activity from ordinary traffic. IoT devices are different from traditional devices [38]. IoT protocols guarantee that the information transferred from endpoint devices, such as sensors, is received and interpreted by another end product, portal, or program. IoT devices communicate differently. Their protocols are different. When an attacker tries to attack an IoT device, it uses a different approach. Communication between these devices is different from traditional devices that's why we need to classify DOS attacks efficiently. Our approach is a multiclassifier system 3 that classifies DOS attacks and normal traffic in IoT devices in a voting-based system. Multiclassifiers could help us classify DOS assaults using machine-learning techniques to detect and improve accuracy. We will tackle the security issue in IoT devices by deploying our machine learning model. The detection of DOS attacks is a crucial topic because they create a serious threat to Internet of Things (IoT) devices. In this study, we provide a multi-classification approach that uses features based on entropy to recognize DOS attacks. In our method, the Shannon entropy is employed to measure the unpredictable nature of the data collection and is extracted from network packet field values. We can identify and look into rapid changes in disorder by monitoring entropy. The most impacted fields are used to concurrently calculate entropy for many IP packet fields. Makes it possible for us to distinguish between various attack kinds. Additionally, we can identify DOS attempts that lower packet randomness by evaluating the randomness variations that occur when an attacker sends similar packets. Three classification models, the Support Vector Machine (SVM), Alternating Decision Tree (ADT), and Multilayer Perceptron (MLP), make up our multi-classification system. These classifiers improve the classification phase's ability to distinguish between normal traffic and a DOS attack. The most recent IoT-based dataset is used to identify recent DOS assaults, and machine learning techniques are used to determine whether or not traffic is safe. We compared the performance of each classifier and discovered that ADtree had the best results. Therefore, we used it to reach our judgment. According to the empirical data in the findings section, predictable traffic is indicated by a lack of classifier agreement, but regular traffic tends to have consistent characteristics. We employ a current dataset from the open-source cybersecurity software developed by the Canadian Institute for Cybersecurity to guarantee the efficacy of our strategy. The collection includes traffic from various IoT devices, such as cameras and home automation systems, gathered using Wireshark and Dumpcap. The communication and behaviors of these IoT devices vary from typical devices, which can impact the attacking strategy, as shown through network traffic analysis. In our multiple-classification system, each classifier provides a conclusion, and the majority judgment is taken into account; however, if there is a tie, no judgment is made. The third classifier ADT serves as the judge who renders the verdict. This strategy for detecting DOS attacks on IoT devices boosts the detection of DOS assaults. The working of the proposed approach is illustrated in the figure 3.

B. Dataset description

We used the Canadian Institute for Cybersecurity’s IoT cybersecurity dataset for the proposed study (CIC). CIC is a well-known organization comprised of internationally recognized researchers and practitioners. The dataset was created for manual behavioural analysis and vulnerability testing of Internet of Things (IoT) devices. The data was collected through gateways using Wireshark, an open-source network protocol analyser. The dataset includes six subdirectories for each trial: power, idle, interaction, scenario, active, and attack experiments. We have used state-of-the-art datasets for profiling, behavioral analysis, and vulnerability testing of IoT devices with different protocols, such as IEEE 802.11, Zigbee-based, and Z-Wave. The following illustrates the main objectives of the CIC IoT Dataset 2022 [39].

- Power: For this experiment, each gadget in the lab was individually turned on, and then a network traffic collection was begun.

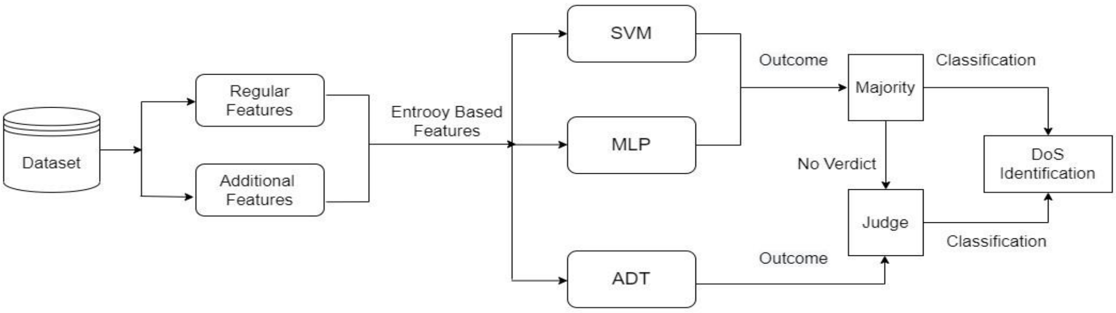


Fig. 3. Multi Classifier system Methodology

-
- Idle: In this experiment, the real network traffic from late at night to early in the morning was recorded. They refer to this period as idle time. The whole lab was evacuated at this time, and no human contact took place.
- Interactions: All conceivable functionality on IoT devices has been extracted for this experiment, and the related network activity and sent packets for each capability/activity have been recorded.
- Scenarios: In these studies, six distinct kinds of scenario tests were carried out utilizing various devices to simulate network activity in a smart home. These tests were conducted to see how several gadgets functioned concurrently.
- Active: The whole network’s communications were recorded throughout the day in addition to the idle period. During this time, all co-workers could come and go from the lab as they pleased. They may engage in active or passive network traffic generation and device interaction.
- Attacks: In this experiment, they carried out two distinct attacks—Flood and RTSP-Brute Force—on a few of our machines and recorded the network data associated with those attacks. They used Wireshark and dumpcap in six different kinds of tests to record the network traffic of the IoT devices passing through the gateway to acquire the data (CIC IoT Dataset 2022)

C. DOS Classification

In our proposed system, when defining a kind of information warfare, a denial-of-service (DOS) assault is carried out when a malicious user prevents legitimate users from accessing network services by using up all of the available resources on the target system. Without obtaining passwords or hacking into the database.

DOS attack traffic is distinguished from normal network traffic using classification. Packet header information, including source IP and destination IP, source port and destination port, protocol, and time-to-live (TTL), is useful for categorizing network traffic [39]. In our case, we have observed that the communication between the attacker and every IoT device differs. When an attacker sends a huge amount of traffic quickly, as shown in the figure, it causes congestion. Where there is normal communication, it is considered as flow, and when there is an anomaly in communication that is consistent too, which is causing congestion is classified as DOS attack by our multiclassifier system Finding the traffic pattern that generates congestion due to an assault and confirming suspected hosts to determine if the host is indeed an attacker is a challenge in providing a robust mechanism against DOS attacks.

1) TCP/ SYN: When a malicious actor launches a DOS attack will flood the network with traffic by launching a flood of requests to the targeted system. The massive overload makes it impossible for any packet to reach its destination. TCP connections are typically formed using a standard three-way handshake. A client sends a SYN packet to the server to establish communication. The server responds to the client's request by delivering a SYN-ACK packet and making buffer space available for the connection. The connection is complete when the client sends back an ACK packet in response. An attacker launches a TCP SYN flood attack when they send many SYN packets to a target. Exchanges of SYN and SYNACK packets, but no final ACK message is ever transmitted to the server. This means the connection is never fully formed, and the server must devote buffer space to accommodate the influx of never-fully established connections. If the attack is successful, the server's buffer will overflow with incomplete connections, making it impossible for legitimate connection requests to be processed. This is an example of a denial of service (DOS) attack, which aims to prevent legitimate users from using the victim's computer system or network resource.

V. MACHINE LEARNING CLASSIFIERS

A. Support Vector Machine

Since our data may be split into two categories—attack and regular traffic we employ a support vector machine (SVM) to do the sorting for us. To classify data, a support vector machine (SVM) 4looks for the optimal hyperplane that divides all points into two distinct classes. For a support vector machine (SVM), the optimal hyperplane is the one that produces the maximum separation between the classes. Margin refers to the maximum width of the slab parallel to the hyperplane for which there are no interior data points. The data points that are on the border of the slab and are closest to the separating hyperplane are the support vectors. These distinctions are shown graphically in the accompanying picture, with" green lock" denoting data points of type 1 (normal traffic) and" black logo" denoting data points of type 2. (attack). Different types of classification is used in the literature [41-44].

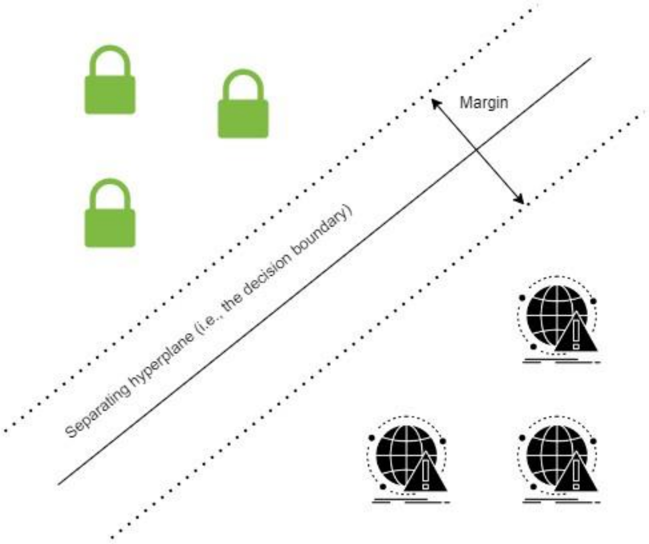


Fig. 4. Support Vector Machine

B. MLP

MLP is an addition to feed-forward neural networks. It comprises three layers: the input, the output, and the hidden. The input layer is responsible for receiving the message. The output layer is for prediction and categorization. The Multilayer Perceptron is taught using the backpropagation learning technique on its neurons. MLPs are intended to approach any continuous function and can tackle nonlinearly distinct issues. MLP's primary applications include pattern categorization, identification, forecasting, and approximations. The feed-forward neural network is supplemented by the multi-layer perceptron (MLP). As can be seen in Fig.5 it has three distinct layers: an input layer, an output layer, and a concealed layer. The signal that is to be processed enters the network at the input layer. The output layer is responsible for completing tasks like prediction and categorization. The real computational engine of the MLP is an arbitrary number of hidden layers positioned between the input and output layers. In an MLP, data moves from the input layer to the output layer, just as it would in a feed-forward network. When it comes to training the MLP's neurons, the backpropagation learning technique is used. Problems that cannot be solved by linearly separating the variables are well within the capabilities of MLPs, which are intended to approximate any continuous function. Classification, identification, prediction, and approximation of attack patterns are among MLP's most common applications, required by us [40]. MLP Countermeasures for Denial of Service attacks are most effective when deployed close to the attack source, at the network's edge. Because congestion isn't the defining anomalous characteristic for DOS, it's difficult to detect them by monitoring an over-provisioned backbone connection near the source or the victim. Most analyses use the MLP's efficiency to zero down on a single detection parameter that accurately flags DDOS assaults. It is the study of how basic models of biological brains may be utilized to address complex computing problems, such as the predictive modeling problems encountered in machine learning. The objective is not to produce realistic brain models but rather to develop robust algorithms and data structures that may be used to simulate complex situations.

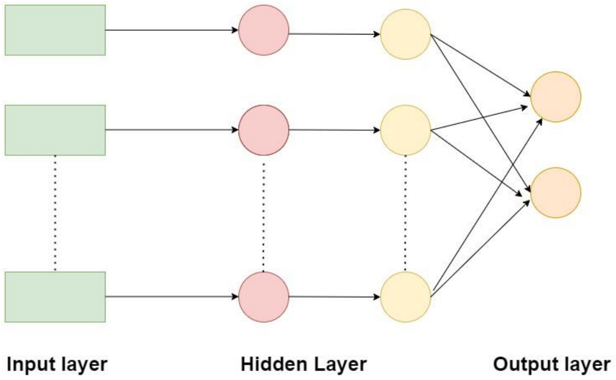


Fig. 5. Multil Layer Perceptron

C. Alternating Decision Tree

Alternating Decision Tree is a subclass classification model that generalizes the Decision Tree. ADTree 6 is a valuable extension of enhancing the decision tree framework. It enables the adaption of various boosting strategies to construct an ADTree model with unique properties capable of handling a variety of uses. The technique of machine learning known as an ADTree alternates between two decision trees. It has ties to boosting and generalizes decision trees. Decision nodes, which define a predicate condition, are interspersed with prediction nodes, which hold a single number, to form an ADTree.

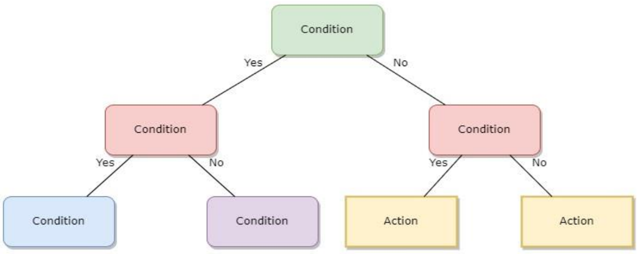


Fig. 6. Alternating Decision Tree

In order to assign a classification to a given instance, an AD Tree takes into account the truth of each prediction node along each route that leads to a decision node. Data-driven decision tree learning is a challenging optimization issue. The most used technique, which dates back to the 1980s, is based on a greedy development of the tree structure by recursively separating nodes and sometimes trimming the final tree. By reducing an impurity measure, an internal node's parameters (decision function) are roughly determined.

VI. EXPERIMENTATION AND RESULTS

The outcomes of our experiments with the proposed method are discussed in this section. Performance is measured in a variety of ways. They begin with a comprehensive evaluation of all classifiers across various performance metrics. Classifiers were evaluated regarding their ability to detect actual attacks, the number of TPRate, FPRate, Precision, Recall, F-Measure, MCC, ROC Area, and PRC Area are covered. Furthermore, these findings were compared to those in the underlying publication

A. Experimental Setup

Our Approach is based on the classification of DOS attacks on IoT devices. We have used a Lenovo Carbon X1 i7 6th generation laptop which has specifications of 8 GB ram, quad core CPU, and m2 SSD. We have run multiple software and tools to implement our Approach. We are using an open-source dataset from the Canadian Institute for Cybersecurity, downloaded free from their website.

B. Practical Implementation

We have implemented our Multiclassification system in the CIC IoT 2022 dataset in a way that: A Figure describes how we implemented our DOS detection system [45]. First of all, there is, raw data is obtained from CIC open-source website. The dataset is in a Pcap file; at first, we need to convert it into a CSV file; meanwhile, we analyzed the communication between the IoT device and the attacker in the form of network packets. For analyzing network traffic packets one by one, we have used Wireshark and Network Miner After the raw data, we have converted it to CSV format. We cleaned this CSV data by removing noise i-e inverted commas, extra-space, empty cell, etc as shown in figure:8

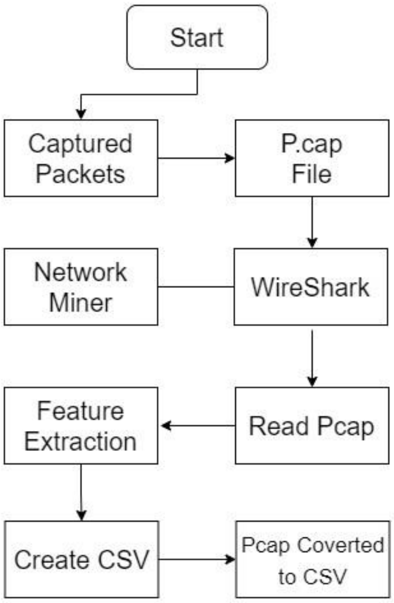


Fig. 7. Implementation Details

C. Pre Processing

We conducted the pre-processing step. The next stage is cleaning the dataset, which involves removing things like noise, unnecessary space, and errant commas or slashes. Then we extracted entropy-based features from the dataset. The feature extraction section describes a detailed discussion of the data extraction. For traffic analysis, we have analysed all the packets individually to see how they behave. For each packet's information and details, we have used network miner 9and wire shark10.

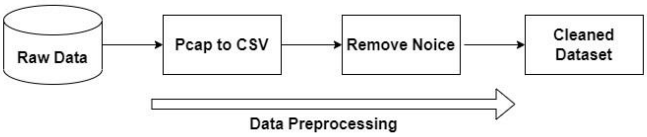


Fig. 8. Data Pre-processing steps

They are very useful, especially Wireshark 9 because we have found a majority and vital information from the Wireshark software shown in Figure 10. In the Packet analysis step, we have discovered the following information shown in the figure. This figure shows that there is a sudden increase in traffic. After analyzing all the traffic and understanding the communication between an attacker and a device, we can label the dataset.

Machine learning systems usually need a lot of data to build a solid foundation for accurate learning patterns. So that the model can sort the data into patterns that give the desired answer, the data used to guide learning must be labeled or annotated based on data characteristics. To make a good algorithm, the labels used to describe the characteristics of the data should be informative, differentiating, and independent.

Correctly labeled data gives the machine learning model something to compare its predictions to ensure they are right and help it improve. A good algorithm is both very accurate and of high quality. One way to determine how accurate a dataset is is to see how close some of its labels are to the real thing. The overall reliability of a set of data is a good way to judge its quality. Over 80 percent of the time businesses spend on AI initiatives is spent on data preparation, cleaning, and labeling, according to a new analysis from AI research and consultancy company Cognilytica. Classification After dataset labeling, we moved to the next step, classification, in which we did model training in a way that we applied our multi-classifier system. We implemented our technique in an Open Source software, weka. As discussed in the methodology figure 3, we have used three classifiers, SVM, MLP, and AD tree, in a majority voting-based strategy. After doing all the work, we generated the results in the form of True Positive, False Positive, Precision, recall, F measure, and Roc area. All our implementation steps are shown in the figure

D. Feature Extraction

Entropy is a fundamental concept in information theory because it measures the uncertainty in network data. when more helpful characteristics for traffic categorization. The entropy rate is lowered when the class distribution is pure; it only belongs to one class. When the class distribution is impure, the entropy rate increases when it contains multiple classes. A way to find changes in randomness is to compare the rate of entropy of one sample of packet header fields to another instance. Entropy measurements are techniques to quantify the unpredictability of some raw traffic characteristics. Characteristics provide a different perspective of the network traffic, revealing the variances in the raw traffic parameters. Features are essential for attack identification. Attributes from the collected datasets were extracted using Wireshark and Network Miner software. The data was saved in a CSV file for" comma-separated values." We build two different entropy-based features. Raw traffic information like IP addresses, port numbers, and protocol numbers are transformed into entropy-based features by applying an entropy measure. In the case of entropy based on source address, for instance, a high number suggests a great deal of diversity in the sources of the traffic packets, whereas a low value indicates less variation. We use two distinct feature sets to categorize traffic better. Traditional entropy-based features are often employed for traffic categorization, and one example is the 5-tuple feature (Source IP address, Destination IP address, Source port, Destination port, and Protocol) these 5-tuple features are our regular features, and in addition, we added more features. We can increase the generality of detecting various DOS assaults if we have more helpful information for traffic

1) Source IP
2) Destination IP
3) Protocol
4) Src port
5) Dst port

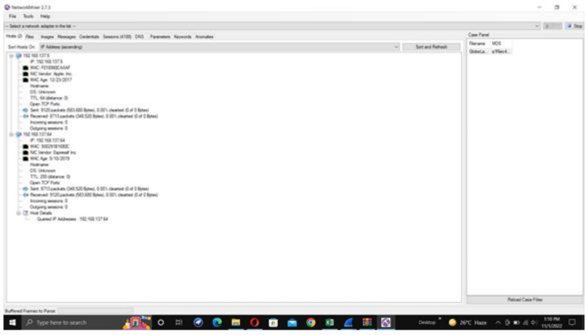
categorization. Features used in our implementation are listed below. A typical DDOS assault with many attack sources targeting a single or limited group of devices has a higher variance in the source IP addresses and a lower variation in destination IP addresses than regular traffic. Entropy-based solutions are usually easy to compute, have high sensitivity, and are independent of network use. However, most current techniques rely on a restricted collection of entropy-based detection characteristics that are only useful for DDOS attacks and may fail to identify other types of DDOS attacks effectively. Selecting the optimal collection of entropy-based features to identify all sorts of DDOS attacks is a challenging challenge that requires an in-depth analysis of each feature and its efficacy in separating the attack traffic from regular traffic. In addition, it is essential to comprehend the influence of entropy measures and window size used in creating entropy-based features on the efficacy of detecting DDOS attacks, exceptionally high- and low-intensity DDOS attacks.

1) Number
2) Time
3) packet Length (bytes)
4) frame.time epoch
5) tcp.seq
6) tcp.ack
7) tcp.window size
8) tcp.window size value
9) frame.coloring rule. name
10) tcp.stream

11) tcp.len
12) frame.time relative

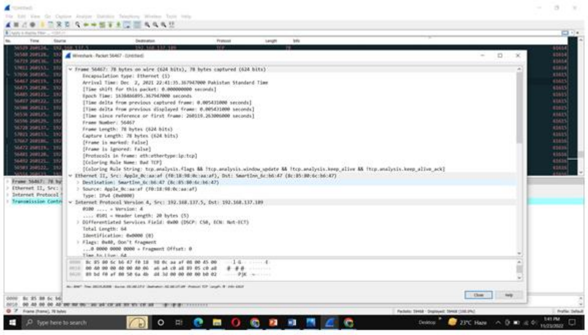
E. DOS Classification

When defining a kind of information warfare, a denial-of-service attack is carried out when a malicious user prevents legitimate users from accessing network services by using up all of the available resources on the target system. Without obtaining passwords or hacking into the database. DOS attack traffic is distinguished from normal network traffic using classification. Packet header information, including source IP and destination IP, source port and destination port, protocol, and time-to-live (TTL), is useful for categorizing network traffic. In our case, we have observed that the communication between the attacker and every IoT device differs. When an attacker sends a huge amount of traffic quickly, as shown in the figure, it causes congestion. Where there is normal communication, it is considered as flow, and when there is an anomaly in communication that is consistent too, which is causing congestion is classified as a DOS attack by our multiclassifier system Finding the traffic pattern that generates congestion due to an assault and confirming suspected hosts to determine if the host is indeed an attacker is a challenge in providing a robust mechanism against DOS attacks.



```
192.168.137.5
    IP: 192.168.137.5
    MAC: F018980CAAAF
    NIC Vendor: Apple, Inc
    MAC Age: 12/23/2017
    Hostname:
    OS: Unknown
    TTL: 64 (distance: 0)
    Open TCP Ports:
    Sent: 9120 packets (583,680 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 8713 packets (348,520 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 0
192.168.137.64
    IP: 192.168.137.64
    MAC: 5002918168DC
    NIC Vendor: Espressif Inc.
    MAC Age: 5/10/2019
    Hostname:
    OS: Unknown
    TTL: 255 (distance: 0)
    Open TCP Ports:
    Sent: 8713 packets (348,520 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 9120 packets (583,680 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 0
    Host Details
        Queried IP Addresses : 192.168.137.64
```

NetworkMiner 2.7.3
File Tools Help
-- Select a network adapter in the list --
Hosts (2) Files Images Messages Credentials Sessions (4100) DNS Parameters Keywords Anomalies
Sort Hosts On: IP Address (ascending)
Sort and Refresh
Case Panel
Reload Case Files
Buffered Frames to Parse:



```
Frame 56467: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec  2, 2021 22:41:35.367947000 Pakistan Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1638466895.367947000 seconds
    [Time delta from previous captured frame: 0.005431000 seconds]
    [Time delta from previous displayed frame: 0.005431000 seconds]
    [Time since reference or first frame: 260119.263006000 seconds]
    Frame Number: 56467
    Frame Length: 78 bytes (624 bits)
    Capture Length: 78 bytes (624 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: Bad TCP]
    [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack]
Ethernet II, Src: Apple_0c:aa:af (f0:18:98:0c:aa:af), Dst: SmartInn_6c:b6:47 (8c:85:80:6c:b6:47)
  > Destination: SmartInn_6c:b6:47 (8c:85:80:6c:b6:47)
  > Source: Apple_0c:aa:af (f0:18:98:0c:aa:af)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.137.5, Dst: 192.168.137.189
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 64
    Identification: 0x0000 (0)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
```

Fig. 9. Analysis in Network Miner Fig. 10. Analysing traffic in Wireshark

F. TCP SYN Attack

When a malicious actor launches a DOS attack will flood the network with traffic by launching a flood of requests to the targeted system. The massive overload makes it impossible for any packet to reach its destination. TCP connections are typically formed using a standard three-way handshake. A client sends a SYN packet to the server to establish communication. The server responds to the client’s request by delivering a SYN-ACK packet and making buffer space available for the connection. The connection is complete when the client sends back an ACK packet in response. An attacker launches a TCP SYN flood attack when they send many SYN packets to a target. Exchanges of SYN and SYN-ACK packets, but no final ACK message is ever transmitted to the server. This means the connection is never fully formed, and the server must devote buffer space to accommodate the influx of connections that are never fully established. If the attack is successful, the server’s buffer will overflow with incomplete connections, making it impossible for legitimate connection requests to be processed. This is an example of a denial of service attack, which aims to prevent legitimate users from using the victim’s computer system or network resource shown in Figure 11.

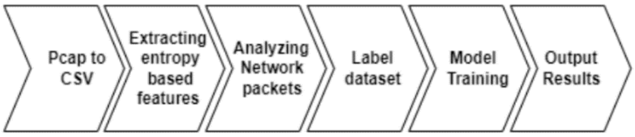


Fig. 11. Implementation steps

G. Experimental Setup

Our Approach is based on the classification of DOS attacks on IoT devices. We have used a Lenovo Carbon X1 i7 6th generation laptop which has specifications of 8 GB RAM, quad-core CPU, and m2 SSD. We have run multiple software and tools to implement our Approach. We are using an open-source dataset from the Canadian Institute for Cybersecurity, downloaded free from their website.

VII. RESULTS

The results part is a section where the key discoveries of our study are described. The comparative performance study of Entropy-based Detection of IoT-based DOS attacks utilizing Multi-Classifiers is shown in Figures 12, 13, 14, and 15. TPRate, FPRate, Precision, Recall, F-Measure, MCC, ROC Area, and PRC Area are used to quantify performance. The findings show that Entropy-based Detection with MultiClassifiers performs well for other competitive values.

A. Eufy Home Base

Our method was put into practice using the CIC IoT 2022 dataset, which contains a number of IoT devices connected to cameras and home automation that we individually built in a single device, the Eufy Home Base.

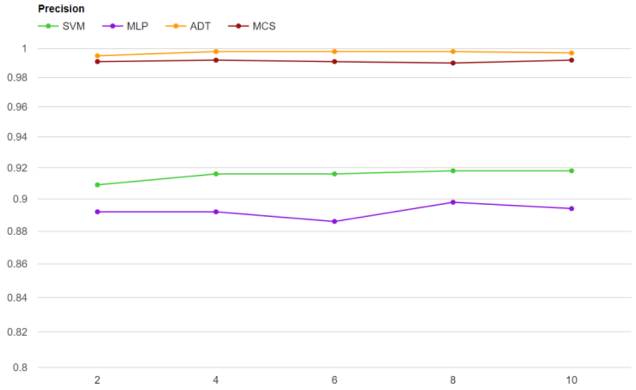


Fig. 12. Precision Eufy Home Base

Here are our findings: First, we used a method known as” Cross-validation Fold” to create a large number of subsets of the original training data.

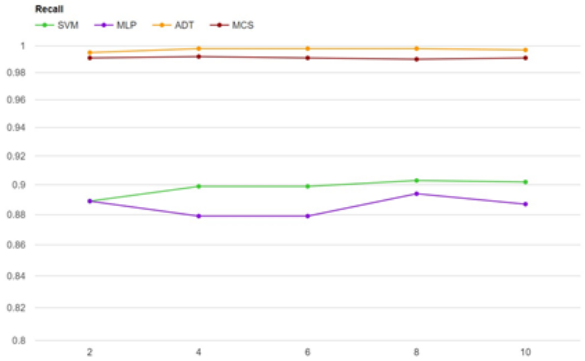


Fig. 13. Recall Eufy Home Base

Our model run 5 times which is shown in the graph, In the Figure X axis there is Kfold and in the Y axis, there is the results percentage. We performed our experiments by using three classifiers individually and also by our proposed multiclassifier system.

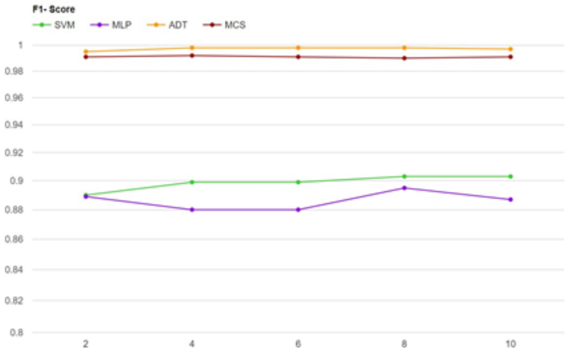


Fig. 14. F1 score Eufy Home Base

The number of Precision, Recall, F-Measure, and ROC Area are covered. Classifiers were assessed in terms of their capacity to identify real assaults. Additionally, these results were contrasted in the graph.

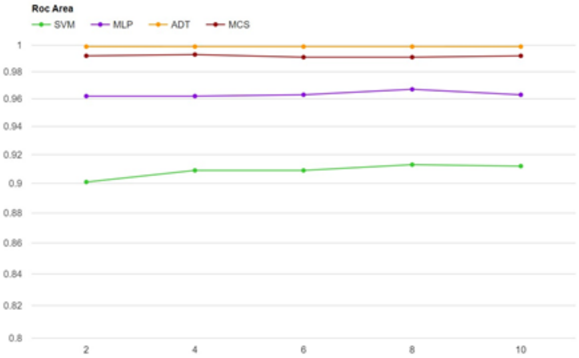


Fig. 15. Roc Area Eufy Home Base

B. ArloQcam

Our method was put into practice using the CIC IoT 2022 dataset, which contains a number of IoT devices connected to
cameras and home automation that we individually built in a
single device, the ArloQcam.

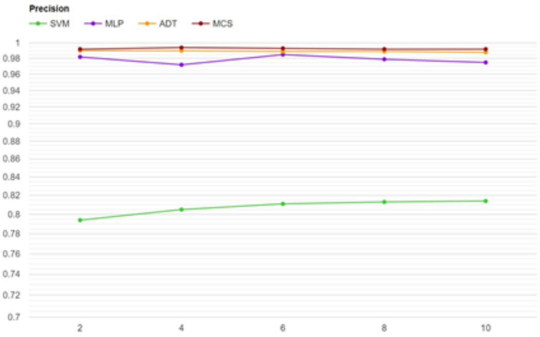


Fig. 16. Precision ArloQcam

Here are our findings: First, we used a method known as” Cross-validation Fold” to create a large number of subsets of the original training data.

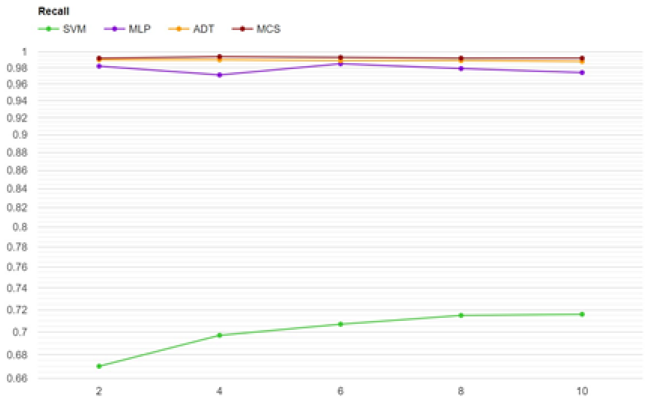


Fig. 17. Recall ArloQcam

Our model run 5 times which is shown in the graph, In the Figure X axis there is Kfold and in the Y axis, there is the results.

percentage. We performed our experiments by using three classifiers individually and also by our proposed multiclassifier system.

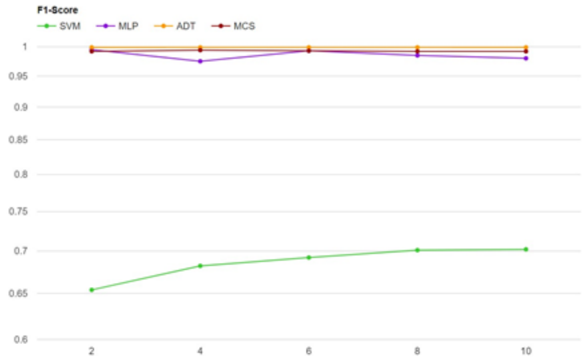


Fig. 18. F1 score ArloQcam

The number of Precision 16, Recall 17, F-Measure 18, and ROC Area 19 are covered. Classifiers were assessed in terms of their capacity to identify real assaults. Additionally, these results were contrasted in the graph.

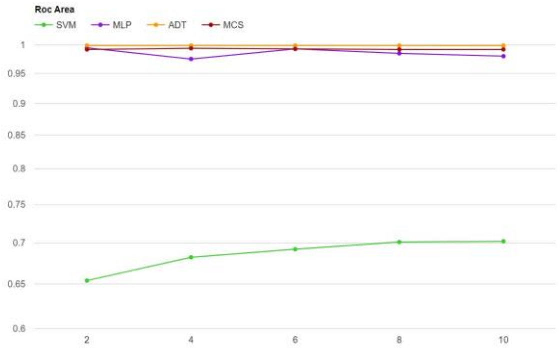


Fig. 19. Roc Area ArloQcam

VIII. COMPARISON WITH OTHER APPROACHES

In Table, we also illustrate how our method stacks up against similar, contemporary, and existing entropy-based methods. Results were also compared to those obtained using a different, more modern method, 10-fold cross-validation, which had been used in Earlier Studies as a benchmark for us that's why we used Kfold 10 and compared it with it as shown in Table 3.

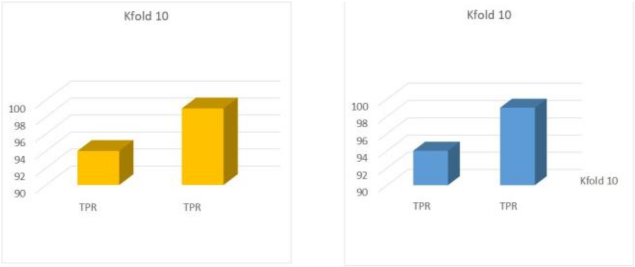


Fig. 20. Implementation steps

Based on the evaluation findings, our technique beat entropy-based methods as well as other cutting-edge methods, including those based on entropy-based approaches. In comparison to prior studies that only included data from conventional devices, our method improved accuracy by 4.36 and 4.37 percentage points. In addition, our method has been implemented on two IoT devices which are Arlo Cam and Eufy Home Automation. We have shown the working of entropy-based approaches on IoT datasets as these devices are different from traditional devices.

TABLE III COMPARISON WITH OTHER APPROACH

Approaches	MultiClassifier	MultiClassifier
Type	Base Paper	Our Paper
Cross Validation	KFold-10	KFold-10
TPR	94.74	99.1 and 99.2

IX. CONCLUSION

To test our strategy, we conducted several DOS assault trials using actual data. To detect DOS attacks on IoT devices, we evaluate our entropy-based parameter's efficacy and employ Multi-Classifiers. Our findings suggest that features retrieved using an entropy-based method with several classifiers are adequate and have effectively mitigated the attack. We used a multi-classifier system to characterize a feature based on entropy. To evaluate our method's efficacy, we calculate entropy using a variety of packet field characteristics. Tests show that the evaluated approach effectively labels different types of DOS assaults. Several kinds of DOS assaults are visible in our approach. Through a variety of methods, we put our strategy into action. We first tried our method in ArloQcam to see how a single device reacts to a denial-of-service attack. When we implemented our approach in the Eufy Home Automation Dataset, we obtained better results. We obtained encouraging proof of the suggested method's efficacy. To test the efficacy of our approach, we ran a battery of tests using the CIC IoT 2022 dataset for various devices. We evaluate our suggested method's efficacy using a single device and a set of devices, and we draw conclusions based on our findings. Based on the data we collected and analyzed, we found that each kind of IoT device has its unique pattern of behavior.

X. FUTURE WORK

The following parameters might be potential future work. Future IoT devices' DDOS attack performance may be accurately improved by evaluating other detection techniques suggested in the literature. The upgraded version of Entropy-based Detection utilizing Multi-Classifiers computation may be used in real-world processing. Additionally, several attack kinds must be put to the test to gauge their effectiveness. To more accurately assess our technique, an expanded experiment may be performed.

Conflicts of interest or competing interests

The authors have no relevant financial or non-financial interests to disclose. The authors have no conflicts of interest to declare that are relevant to the content of this article.

REFERENCES

[1]. Kölbl, Stefan, Elmar Tischhauser, Patrick Derbez, and Andrey Bogdanov. "Troika: a ternary cryptographic hash function." Designs, Codes and Cryptography 88, no. 1 (2020): 91-117.

[2]. A. Praseed and P. S. Thilagam, “DDOS attacks at the application layer: Challenges and research perspectives for safeguarding web applications,” IEEE Communications Surveys Tutorials, vol. 21, no. 1, pp. 661–685, 2018.

[3]. R. Vishwakarma and A. K. Jain, “A survey of dDOS attacking techniques and de- fence mechanisms in the iot network,” Telecommunication systems, vol. 73, no. 1, pp. 3–25, 2020.

[4]. S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (dDOS) flooding attacks,” IEEE communications surveys tutorials, vol. 15, no. 4, pp. 2046–2069, 2013.

[5]. A. O. Prokofiev and Y. S. Smirnova, “Counteraction against internet of things botnets in private networks,” in 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 301–305, IEEE, 2019.

[6]. S. Chesney, K. Roy, and S. Khorsandroo, “Machine learning algorithms for pre- venting iot cybersecurity attacks,” in Proceedings of SAI Intelligent Systems Confer- ence, pp. 679–686, Springer, 2020.

[7]. https://www.nist.gov/blogs/cybersecurity-insights/more-just-milestonebotnet- roadmap-towards-more-securable-iot-device 2022.

[8]. S. A. Kumar, T. Vealey, and H. Srivastava, “Security in internet of things: Chal- lenges, solutions and future directions,” in 2016 49th Hawaii International Conference on System Sciences (HICSS), pp. 5772–5781, IEEE, 2016.

[9]. I. Ahmad, M. S. Niazy, R. A. Ziar, and S. Khan, “Survey on iot: security threats and applications,” Journal of Robotics and Control (JRC), vol. 2, no. 1, pp. 42–46,2021.44

[10]. A. Koay, A. Chen, I. Welch, and W. K. Seah, “A new multi classifier system using entropy-based features in dDOS attack detection,” in 2018 International Conference on Information Networking (ICOIN), pp. 162–167, IEEE, 2018.

[11]. Y. Tao and S. Yu, “DDOS attack detection at local area networks using information theoretical metrics,” in 2013 12th IEEE international conference on trust, security and privacy in computing and communications, pp. 233–240, IEEE, 2013.

[12]. X. Ma and Y. Chen, “DDOS detection method based on chaos analysis of network traffic entropy,” IEEE Communications Letters, vol. 18, no. 1, pp. 114–117, 2013.

[13]. R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del Rincon, and D. Siracusa, “Lucid: A practical, lightweight deep learning solution for dDOS at- tack detection,” IEEE Transactions on Network and Service Management, vol. 17, no. 2, pp. 876–889, 2020.

[14]. N. Abughazaleh, R. Bin, and M. Btish, “DOS attacks in iot systems and proposed solutions,” Int. J. Comput. Appl., vol. 176, no. 33, pp. 16–19, 2020.

[15]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[16]. J. Bhayo, S. Hameed, and S. A. Shah, “An efficient counter-based dDOS attack detection framework leveraging software defined iot (sd-iot),” IEEE Access, vol. 8, pp. 221612–221631, 2020.

[17]. Y. N. Soe, P. I. Santosa, and R. Hartanto, “DDOS attack detection based on simple ann with smote for iot environment,” in 2019 Fourth International Conference on Informatics and Computing (ICIC), pp. 1–5, IEEE, 2019.

[18]. H. k. Idriss, “Mirai botnet in lebanon,” in 2020 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–6, 2020.

[19]. M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, “Use of honeypots for mit- igating DOS attacks targeted on iot networks,” in 2017 International conference on computer, communication and signal processing (ICCCSP), pp. 1–4, IEEE, 2017.

[20]. R. Vishwakarma and A. K. Jain, “A honeypot with machine learning based de- tection framework for defending iot based botnet dDOS attacks,” in 2019 3rd Inter- national Conference on Trends in Electronics and Informatics (ICOEI), pp. 1019–1024, IEEE, 2019. 45

[21]. B. Wang, Y. Dou, Y. Sang, Y. Zhang, and J. Huang, “Iotcmal: Towards a hybrid iot honeypot for capturing and analyzing malware,” in ICC 2020-2020 IEEE Interna- tional Conference on Communications (ICC), pp. 1–7, IEEE, 2020.

[22]. N. Ravi and S. M. Shalinie, “Learning-driven detection and mitigation of dDOS attack in iot via sdn-cloud architecture,” IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3559–3570, 2020.

[23]. A. Munshi, N. A. Alqarni, and N. A. Almalki, “DDOS attack on iot devices,” in 2020 3rd International Conference on Computer Applications and Information Security (ICCAIS), pp. 1–5, IEEE, 2020.

[24]. M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, “Iot sentinel: Automated device-type identification for security enforcement in iot,” in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 2177–2184, IEEE, 2017.

[25]. Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, “Fog-assisted sdn controlled framework for enduring anomaly detection in an iot network,” IEEE Access, vol. 6, pp. 73713–73723, 2018.

[26]. J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, “Cnn-based network intrusion detection against denial-of-service attacks,” Electronics, vol. 9, no. 6, p. 916, 2020.

[27]. B. H. Ali, N. Sulaiman, S. A. R. Al-Haddad, R. Atan, S. L. M. Hassan, and M. Al- ghrairi, “Identification of distributed denial of services anomalies by using combi- nation of entropy and sequential probabilities ratio test methods,” Sensors, vol. 21, no. 19, p. 6453, 2021.

[28]. S.-J. Choi and J. Kwak, “A study on reduction of dDOS amplification attacks in the udp-based cldap protocol,” in 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), pp. 1–4, IEEE, 2017.

[29]. Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, “Flowguard: an intelligent edge defense mechanism against iot dDOS attacks,” IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552–9562, 2020.

[30]. N. Chand, P. Mishra, C. R. Krishna, E. S. Pilli, and M. C. Govil, “A comparative analysis of svm and its stacking with other classification algorithm for intrusion detection,” in 2016 International Conference on Advances in Computing, Communication, Automation (ICACCA)(Spring), pp. 1–6, IEEE, 2016.

[31]. R. R. Robinson and C. Thomas, “Ranking of machine learning algorithms based on the performance in classifying dDOS attacks,” in 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp. 185–190, IEEE, 2015.46

[32]. S. A. R. Shah and B. Issac, “Performance comparison of intrusion detection sys- tems and application of machine learning to snort system,” Future Generation Computer Systems, vol. 80, pp. 157–170, 2018.

[33]. M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, “DDOS defense by offense,” in Proceedings of the 2006 conference on Applications, technologies,architectures, and protocols for computer communications, pp. 303–314, 2006.

[34]. S. Weerakkody, B. Sinopoli, S. Kar, and A. Datta, “Information flow for security in control systems,” in 2016 IEEE 55th Conference on Decision and Control (CDC), pp. 5065–5072, IEEE, 2016.

[35]. M. Showkatbakhsh, Y. Shoukry, R. H. Chen, S. Diggavi, and P. Tabuada, “An smt- based approach to secure state estimation under sensor and actuator attacks,” in 2017 IEEE 56th Annual Conference on Decision and Control (CDC), pp. 157–162, IEEE,2017.

[36]. Y. Mo, R. Chabukswar, and B. Sinopoli, “Detecting integrity attacks on scada systems,” IEEE Transactions on Control Systems Technology, vol. 22, no. 4, pp. 1396–1407, 2013.

[37]. V. Dutt, Y.-S. Ahn, and C. Gonzalez, “Cyber situation awareness: Modeling the security analyst in a cyber-attack scenario through instancebased learning,” in IFIP Annual Conference on Data and Applications Security and Privacy, pp. 280–292, Springer, 2011.

[38]. A. Bremler-Barr, H. Levy, and Z. Yakhini, “Iot or not: Identifying iot devices in a short time scale,” in NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, pp. 1–9, IEEE, 2020.

[39]. S. Dadkhah, H. Mahdikhani, P. K. Danso, A. Zohourian, K. A. Truong, and A. A. Ghorbani, “Towards the development of a realistic multidimensional iot profiling dataset,” in 2022 19th Annual International Conference on Privacy, Security Trust (PST), pp. 1–11, IEEE, 2022.

[40]. R. DOShi, N. Apthorpe, and N. Feamster, “Machine learning dDOS detection for consumer internet of things devices,” in 2018 IEEE Security and Privacy Workshops (SPW), pp. 29–35, IEEE, 2018.

[41]. Islam, M. Shujah, Khush Bakhat, Mansoor Iqbal, Rashid Khan, ZhongFu Ye, and M. Mattah Islam. "Representation for action recognition with motion vector termed as: SDQIO." Expert Systems with Applications 212 (2023): 118406.

[42]. Bakhat, Khush, Kashif Kifayat, M. Shujah Islam, and M. Mattah Islam. "Katz centrality based approach to perform human action recognition by using OMKZ." Signal, Image and Video Processing 17, no. 4 (2023): 1677-1685.

[43]. Islam, M. Shujah, Khush Bakhat, Rashid Khan, Nuzhat Naqvi, M. Mattah Islam, and Zhongfu Ye. "Applied human action recognition network based on SNSP features." Neural Processing Letters 54, no. 3 (2022): 1481-1494.

[44]. Bakhat, Khush, Kashif Kifayat, M. Shujah Islam, and M. Mattah Islam. "Human activity recognition based on an amalgamation of CEV & SGM features." Journal of Intelligent & Fuzzy Systems Preprint (2022): 1-12.

[45]. J. N. Bakker, B. Ng, and W. K. Seah, “Can machine learning techniques be ef- fectively used in real networks against dDOS attacks?,” in 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–6, IEEE, 2018.