Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 4, 2026

FEATURE SELECTION BASED LIGHTWEIGHT IDS FOR RESOURCE CONSTRAINED IOT: A COMPREHENSIVE SURVEY

[*1]Dr. Mahawish Fatima, [2]Dr. Osama Rehman, [3]Muhammad Hassan Nasir, [4]Dr. Muhammad Ashraf, [5]Dr. Hina Shakir, [6]Dr. Bushra Fazal Khan, [7]Dr. Muhammad Hussain

*[*1]Assistant Professor, Department of Software Engineering, Bahria University Karachi Campus, Pakistan*
[2]Senior Lecturer, School of Computer Science, Taylor's University, Subang Jaya, Malaysia
[3]Manager I.T, Department of Computer Science & IT, NED University of Engineering & Technology, Pakistan
[4]Associate Professor, Department of Computer Engineering, BUITEMS, Quetta, Pakistan
[5]Associate Professor, Department of Software Engineering, Bahria University Karachi Campus, Pakistan
[6]Assistant Professor, Department of Software Engineering, Bahria University Karachi Campus, Pakistan
[7]Associate Professor, Department of Software Engineering, Bahria University Karachi Campus, Pakistan

*[*1]mahwishfatima.bukc@bahria.edu.pk, [2]Osama.Rehmen@taylors.edu.my*
[3]Mhassan.cse@gmail.com, [4]Muhammad.ashraf@buitms.edu.pk, [5]hinashakir.bukc@bahria.edu.pk
[6]bushrafazal.bukc@bahria.edu.pk
[7]engr.m.hussain.bukc@bahria.edu.pk

Keywords
DoS/DDoS attack, Internet of Things, Network Security, Machine Leaning

Article History
Received on 24 March, 2026
Accepted on 20 April, 2026
Published on 21 April, 2026

Corresponding Author:
Dr. Mahawish Fatima

Abstract
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are of significant importance in the field of cybersecurity, as the threat posed by these attacks continues to increase each year. These attacks particularly exploit Internet of Things (IoT) environment, as IoT networks are often consist of devices with limited computational resources. The rapid proliferation of IoT devices, combined with their inherent resource constraints, makes them an easy target for launching DoS/DDoS attacks. Understanding the severity and exploitation of these attacks, this study presents a comprehensive survey and analysis focusing on DoS/DDoS attacks, including an in-depth discussion of their types within the IoT context. The study highlights the inherent characteristics of IoT systems, particularly resource limitations such as limited processing power, memory, and energy in IoT devices. Furthermore, this work explores Intrusion Detection Systems (IDS) and recent

advancements in attack detection followed by Machine Learning (ML) techniques used for detecting DoS/DDoS attacks. This survey also examines state-of-the-art ML-based lightweight IDS for DoS/DDoS detection. Finally, this paper discusses future research directions required for designing effective DoS/DDoS attack mitigation solutions for resource constrained IoT systems.

1. Introduction

A Denial of Service (DoS) attack floods the target system with an enormous number of packets that contain fraudulent requests, which causes the system to become occupied with handling such illegitimate traffic and fail to address the genuine user service requests (Salim, Rathore et al. 2020). In a similar fashion, a Distributed Denial of Service (DDoS) attack also leverages a massive number of compromised devices for the purpose of overwhelming a target system/network. The attacking individual's control devices and instruct them on how to send a massive amount of fake requests towards the target resulting in the inability to differentiate between genuine and fake traffic.

IoT devices are resource-constrained in terms of CPU and power consumption to fulfill particular tasks. Examples of resource-constrained devices include smart thermostats, security cameras, and health monitors. Because of these constraints, the vulnerability of IoT devices to DoS/DDoS attacks increases to a larger extent. In a DoS/DDoS attack, it has been noticed that the targeted IoT devices might become non-functional and enter a state of abnormal or dysfunctional behavior (Aminu Ghali, Ahmad et al. 2020).

For example, a temperature-control system might not be capable of controlling the temperature in the desired range; a security camera might neither record nor broadcast; and a health monitor might generate invalid readings or become totally non-functional (Moore, Nugent et al. 2020).

With the wide implementation of IoT technology, maintaining the confidentiality, integrity, and availability of computer systems and networks has become a pressing issue. IoT technology possesses naturally vulnerable capabilities that attract attacks from malicious actors. To mitigate these risks, Intrusion Detection Systems (IDS) have been widely investigated. Traditional IDS techniques, however, are often resource-intensive and unsuitable for deployment in IoT environments (Fatima, Rehman et al. 2024). As a result, the research community has focused on lightweight IDS solutions, leveraging feature selection and ML techniques to balance security effectiveness with limited computational resources (Nasir, ZIA et al. 2019). Despite numerous studies in this area, challenges remain, including the detection of emerging attack patterns, the lack of real-world deployment on low-resource devices, and insufficient evaluation of resource utilization metrics such as CPU, memory, and energy consumption (Fatima, Rehman et al. 2024).

This survey provides a comprehensive review of DoS/DDoS attack detection in resource-constrained IoT environments. It systematically examines types of DoS/DDoS attacks, the vulnerabilities of constrained devices, and the current state-of-the-art in lightweight IDS solutions. In addition, it identifies research gaps and emerging challenges, highlighting areas that require further exploration to enhance the security of IoT networks. By synthesizing existing literature, this work aims to provide a holistic understanding of the field, serving as a reference for researchers and practitioners seeking to design effective and resource-efficient IoT security solutions.

Rest of the paper is segmented as follows. Section 2 explains the background and concepts of IoT, DoS/DDoS attacks, machine learning and feature selection. Section 3 discusses security threats and its impact in IoT environment. The section 4 presents the state-of the art within lightweight IDS. The research challenges and gaps are discussed in section 5 followed by conclusion in section 6.

2. Background

2.1 Internet of Things

The Internet of Things (IoT) describes a system of connected devices such as sensors, smart home equipment, wearable technology, and vehicles that can automatically communicate and share data without direct human involvement (Rose, Eldridge et al. 2015). In an IoT architecture, data collection starts at the Perception Layer, which is tasked with detecting and gathering information from the physical world. Devices in this layer monitor environmental and physical conditions, including temperature, humidity, movement, pressure, and geographic location (Rose, Eldridge et al. 2015). After data acquisition, the information is sent to the Network Layer, which acts as the communication backbone of the system, allowing data to move from sensing devices to higher system components. This layer supports multiple communication technologies, including Wi-Fi, Bluetooth, Zigbee, LoRaWAN, and 5G, ensuring reliable data transmission. The data is then delivered to the Application Layer, where advanced processing occurs and meaningful services are provided to end users or organizations through software-based solutions (Mukhopadhyay and Suryadevara 2014). This layer consists of software programs, cloud platforms, and data analytics systems that gather and process the data to produce valuable insights. Together, the Perception, Network, and Application Layers form the essential structure of an IoT system. Each layer serves a distinct purpose collecting, transmitting, analyzing, and acting on data ensuring the system functions smoothly, securely, and with minimal human involvement (Mrabet, Belguith et al. 2020).

Resource Constrained IoT devices

IoT devices are meant to sense the surroundings and communicate the data they have collected. Depending on the purpose of the devices, they may collect data on temperature, motion, and pressure, among other data (Rose, Eldridge et al. 2015). . However, the devices may have limited processing power. This is because the developers have to consider various factors such as the devices' costs, battery lives, sizes, and the purpose of the devices. These factors may affect the devices' ability to run complex programs and provide security features (Mukhopadhyay and Suryadevara 2014)

Table 1: Resource Constrained IoT Gateways

Company	Product	Device Type	Applications	Resources
Milesight	Indoor Ambience Sensor AM100	End Device	Environment	Power: 2 × 2700 mAh Li-SOCl2 replaceable batteries (7–9 Hrs)
	UG63 Mini LoRaWAN Gateway	Gateway		Power: 12000mAh high-capacity battery (up to 32 hours) CPU: ARM Cortex-A7 (528 MHz) Memory: DDR4 RAM (256 MB) + eMMC Flash (4 GB)
AMobile Sol. Corp.	IB003 Smart Water Meter	End Device	Water Supply	Power: AC + Internal Backup Battery (5 days) MCU/CPU: 32-Bit ARM Cortex (480 MHz)
	G350 Gateway	Gateway		Power: DC (12V) CPU: MediaTek 4X Arm Cortex-A53 (2.0 GHz) Memory: RAM (4GB) + Flash (64GB)
Four-Faith	F8914 ZigBee Terminal	End Device	Manufacturing	CPU: Industrial ZigBee Processor
	F-G100 Intelligent Gateway	Gateway		Power: DC (9–36V) CPU: Industrial-grade 32-bit Communication Processor Memory: DDR3 (512MB) + Flash (32MB)
Zoll	Heart Failure Management System	End Device	Healthcare	Power: Rechargeable Battery
	Smartphone-sized Gateway Device	Gateway		Power: Rechargeable Battery (up to 18 Hrs)
Biz4intellia	Intellia Light Sensor INT-Light-02	End Device	Agricultural	Power: 19000mAh Li-SOCl2 battery (up to 5 Years)
	Intellia Indoor LoRaWAN Gateway	Gateway		Power: DC (9–48V) CPU: 64-bit ARM Cortex-A53 (800 MHz) Memory: DDR3 RAM (512 MB) + Flash eMMC (8 GB)

As a result, devices with low processing capacity can be more vulnerable to cyber attacks and may struggle to detect or respond to threats quickly. To show the limitations vary across devices, Table 1 lists examples of IoT end devices and gateway devices from five different manufacturers. Table 1 is based on information from the companies' official websites, compares devices according to CPU speed, memory, and power source. While some manufacturers provide complete details, others only share partial information.

In general, IoT end devices have far fewer resources than their gateway counterparts. As shown in Table 1, many of these devices are limited in one or more areas, making them unsuitable for running resource-heavy security solutions, such as traditional IDS/IPS systems. These limitations increase the risk of attacks, as malicious actors can take advantage of the vulnerabilities to carry out serious cyber threats. In addition, many IoT devices rely on communication technologies with limited bandwidthlike Zigbee, Bluetooth Low Energy (BLE), and LoRaWAN, which makes them particularly vulnerable to network-based attacks

2.3. DoS/DDoS Attacks

During a DoS attack, the attacker floods the victim with a large amount of Internet traffic, making the

system unavailable to its users. DoS attacks originate from flooding the victim with traffic from only one source, while DDoS attacks use several compromised hosts, called bots, to flood the victim concurrently (Khader and Eleyan 2021). DDoS attacks have become common, even targeting multinational corporations of colossal size. An example of this threat was the biggest recorded DDoS that specifically attacked Amazon Web Services (AWS) in February 2020 Effects of DDoS attacks include significant reduction in volume of legitimate traffic, loss of business opportunities, tarnishing of image, etc. (Kumari and Jain 2023), (Sharif, Beitollahi et al. 2023), (Khan, Murphy et al. 2009). Several strategic advantages of DDoS attacks can be listed with regard to their distributed nature

- ***Increased Disruptive Potential:*** This is due to the fact that more machines are being utilized, and therefore, the adversary is in a position to launch more disruptive attacks, thus overwhelming the resources of the target and eventually leading to a high level of service disruption or denial.
- ***Anonymity and Complexity:*** The random spread of attacking hosts can extend globally, including legal hosts as it becomes hard to identify the source of the attack.
- ***Difficulty in Mitigation:*** In cases where there are multiple attacking hosts that have to be mitigated and held back from causing harm to a computer system or network.
- ***Obfuscation of the Attacker Identity:*** This, in essence, relates to covering up the identities of attackers through multiple compromised systems, making it hard to identify the source of an attack.

2.4. Machine Learning

ML can be defined as part of AI, and it relates to developing models that can be utilized in learning as well as making decisions on data (Joshi 2020). Unlike traditional computer programming, where computers are programmed to do a particular job, with ML, computers are instead fed with a lot of data with the sole intent of learning (Ojo, Giordano et al., 2018).(Ojo, Giordano et al. 2018). There are three main classes of Machine Learning (ML), and these are: (i) Supervised learning, (ii) Unsupervised learning, (iii) Reinforcement learning. These are techniques that use statistical approaches to construct models that can learn and generalize from data they are exposed (Jordan and Mitchell 2015).

2.4.1. Supervised Learning

Supervised ML techniques require the use of labeled examples where each example is accompanied by a predetermined label. During the learning phase, the ML algorithm connects the features of the examples to the target output labels. This increases the ability of the model to predict the classes of unseen examples rather accurately. In intrusion detection situations, supervised learning is set to play an extremely important part. These kinds of technologies identify known threats by matching traffic with pre-defined signatures of known attacks stored in a database. As new kind of threats emerge at constant intervals, supervised learning techniques always need updating with new signatures to continue their efficiency (Turgunbaev 2024)

2.4.2. Unsupervised Learning

Unlike supervised learning techniques, unsupervised learning works on data without any labeled examples. Instead of discovering patterns based on examples provided, unsupervised learning algorithms aim to discover patterns based on inherent characteristics of patterns. It can be highly beneficial for anomaly-based IDS systems, which require the detection of new threats. By analyzing data points that do not belong to normal

patterns, researchers can notice new patterns of attacks that are not programmed in the IDS system (Turgunbaev 2024).

2.4.3. Reinforcement Learning

Unlike supervised and unsupervised learning methods, Reinforcement Learning (RL) is associated with an agent interacting with its environment whereby it learns from the results associated with its acts. This is accomplished through feedback received by the agent in an environment in the form of rewards or penalties with the aim of maximizing the rewards received by the agent (Joshi 2020). Regarding the intrusion detection system and the ways to defend the system against threats, the application of RL is possible.

2.5. Feature Selection Techniques

Feature selection (FS) methods can be used to improve the efficiency of IDS, as they have been shown to be effective in increasing its efficiency (Velan, Čermák et al. 2015). FS can be defined as a preprocessing optimization method used to select a subset of features that can be considered important in a dataset, thereby eliminating all redundant features used in a classification system to improve the efficiency of IDS.

Feature selection can be used to improve the efficacy of IDS in an IoT network. Note that it takes a longer time to train and test a dataset with a large number of features, as it consumes plenty of computing resources (Junejo and Goh 2016). However, not all of the features of a dataset are always important for attack detection for a particular IDS classification system. Several methods can be employed to reduce the above-discussed issues, and FS techniques can be used as a pre-processing technique for implementing ML algorithms (Pal and Foody 2010), (Cai, Luo et al. 2018). There are normally four steps involved in the FS process, as illustrated in Figure 1. The steps include the creation of a subset of features based on the original features. This subset is then analyzed using an evaluation function that determines the goodness of the subset. After that, the subset undergoes the stopping criterion decision of whether it should be accepted or rejected. There are three basic types of FS approaches: Wrapper, Filter, and Embedded methods Figure 1.

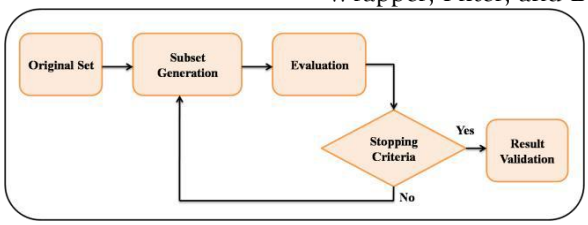

Figure 1: Feature Selection Process

2.5.1. Filter Methods

The filter FS technique removes irrelevant features with less effect on data analysis processes. Filter FS comprises conducting a statistical test on each attribute in the dataset, with primary focus on its correlation with the target variable. According to filter conditions, each feature is assigned ratings based on certain statistical tests (Cai, Luo et al. 2018). Features with the highest ratings are retained, and low-rated features are eliminated. Filter FS is system-resource friendly with low system overhead [98]. Examples of filter FS techniques include Mutual Information (MI), Fisher Score (F-Score), Chi-Square ($\chi 2$), Variance Threshold (VT), Pearson Correlation Coefficient

(R), Mean Absolute Difference (MAD), and Ratio of Dispersion (DR).

2.5.2. **Wrapper Methods**

Wrapper feature selection makes use of the greedy search method that tests all possible feature sets for the chosen evaluation measure (Alamiedy, Anbar et al. 2018). The process analyzes the feature of interest as well as possible feature subsets for the independent variables through the training of the classifier. Even though the accuracy of the method is higher compared to the filter method, the computational cost is higher (Cai, Luo et al. 2018). Examples of the wrapper method include Forward Feature Selection (FFS), Backward Feature Elimination (BFE), and Exhaustive Feature Selection (EFS).

2.5.3. **Embedded Methods**

Embedded techniques merge the strengths of filter and wrapper methods in a way that produces a set of features which are both efficient and very accurate (Chen, Tsai et al. 2020). Embedded FS contrasts with filter and wrapper methods in that embedded FS takes place in tandem with training a model. Embedded methods are therefore more efficient when it comes to resource consumption (Chen, Tsai et al. 2020).

3. Security Threats in IoT

3.1. Attacks in IoT based Systems

The rising use of IoT networks is vulnerable to various cyber-attack types because of their extensive usage and lack of proper security frameworks. These types of cyber-attacks target various layers within the overall architecture that comprises IoT networks. For perception layer, some of the significant risks are related to spoofing, tampering, calibration attacks, sensor nodes, and replay attacks.

In consideration of the network layer, the most common cyber-attacks include Man in the Middle Attacks, DoS/DDoS, Eavesdropping, Traffic Analysis, and Jamming, as discussed in (Humayun, Tariq et al. 2024). In consideration of the application layer, cyber threats include SQL Injection, Cross-Site Scripting, Data Injection, and so on, which include possible cyber threats for unrestricted access to systems, data breaches, and system manipulation, as discussed in (Yoshiyama, Carvalho et al. 1995). The overall scheme of representing different kinds of cyber-attacks within a broader classification of five different parameters is represented in Figure 1 below.

Based on Target: Device-level attack refers to activities like credential theft, firmware tampering, as well as circuit tampering. Network-level attack refers to activities like network interception, network injection, as well as network disruption. This can include activities like data leakage, identity theft, and many more. Data-level attack refers to activities like data breach, damage to the data, and many more, with privacy being the main interest.

Based on Attack Vector: Attacks are categorized into application layer, network layer, and physical layer attacks (Rose, Eldridge et al. 2015). Application-layer attacks comprise Command Injection Attacks, SQL Injection Attacks, and Cross-site Scripting Attacks. Network-layer attacks comprise DoS Attacks, Man-inthe-Middle Attacks, Spoofing Attacks, and Eavesdropping Attacks. Physical-layer attacks comprise Hardware Tampering Attacks and Side-channel Attacks.

Based on Attack Methodology: Shown in Figure 1 identifies active and passive attacks. Active attacks include injection and replay attacks that actively interact with the network. Passive attacks include traffic analysis that involves monitoring information without changing what is happening on the system.

Based on Impact: Attacks are categorized into operational and financial impacts. Operational impacts usually involve disruption and lack of functionality, and can lead to system failure or absence of critical services. But financial impacts involve direct economic losses and reputation damages.

Based on Threat Source: Threat source are categorized into external and internal. External source attacks are usually originated by hackers and cyber-criminals in pursuit of personal agendas. Internal attacks, due to staff members in an organization, usually disgruntled employees seeking to use known vulnerabilities in order to steal or damage data. The need to address these challenges is made more paramount by the increasing convergence of IoT devices with critical and daily life infrastructure. With the rising adoption of IoT technology, there is a critical need for the development and implementation of measures that can protect these devices from threats in their increasing numbers. Such measures must adopt a holistic approach in providing mitigative and detection mechanisms particularly for IoT.

3.2. Impact of DDoS on Computing Resources

In most cases, a DDoS attack depletes the resources of the attacked entity because it floods them with malicious traffic. The vulnerability to the depletion caused by a DDoS attack is especially high in IoT devices due to their inherent limitations in terms of their processing capabilities, including memory. The inherent limitations of the devices make them specially vulnerable to depletion in the event of a DDoS attack.

Table 2 provides a synthesized view of the effects of various forms of DDoS attacks on computer resources such as CPU, memory, and bandwidth. The communication protocols are also mentioned in the Table 2, which are exploited during the attack. A clear understanding of the above is required for an effective method of counteracting the effects of DDoS attacks.

In addition, the table above illustrates the extent to which particular categories of DDoS attacks affect the three main categories of system resources, which are CPU, memory, and bandwidth. For instance, SYN Flood attacks are described as having a high effect on CPU and bandwidth, while having low effects on memory. Such is consistent with the nature of SYN Flood attacks, as they seek to consume the processing capacity of the victim server by generating high volumes of TCP connection requests over the network (Wang, Zhang et al. 2002). Other forms of DDoS attacks, such as HTTP Flood attacks, will put roughly equal amounts of pressure on system CPU, memory, and bandwidth resources, consistent with their complex operation at multiple levels on the protocol stacks (Scheuer, Haase et al. 2011). The table below, Table 2, indicates the normal volume and time for these types of attacks, showing the level at which a DDoS attack may occur. For example, a Domain Name System (DNS) and Network Time Protocol (NTP) attack may be able to create data traffic levels that reach from several hundred Gbps to Tbps, making it one of the most dangerous types of a DDoS attack (Lavrenovs 2023) .

The level at which these types of attacks may be able to continue from minutes to hours contributes to their dangerous level. In particular, it may be seen that although a Slowloris attack may be considered to have a relatively mild level of damage to bandwidth, it may be able to continue from hours to days (Damon, Dale et al. 2012).

With regard to the IoT environment where a regular characteristic of IoT appliances is low processing power and bandwidth capabilities, the relevance of specially designed defense mechanisms is highlighted by Table 2 itself. CPU-intensive attacks like SYN flood attacks and UDP attacks that require a huge amount of bandwidth are a major concern for IoT appliances that could be strained or disabled by such attacks. Also a major concern could be the type of amplification attack that relies on a relatively low request volume but a huge response volume.

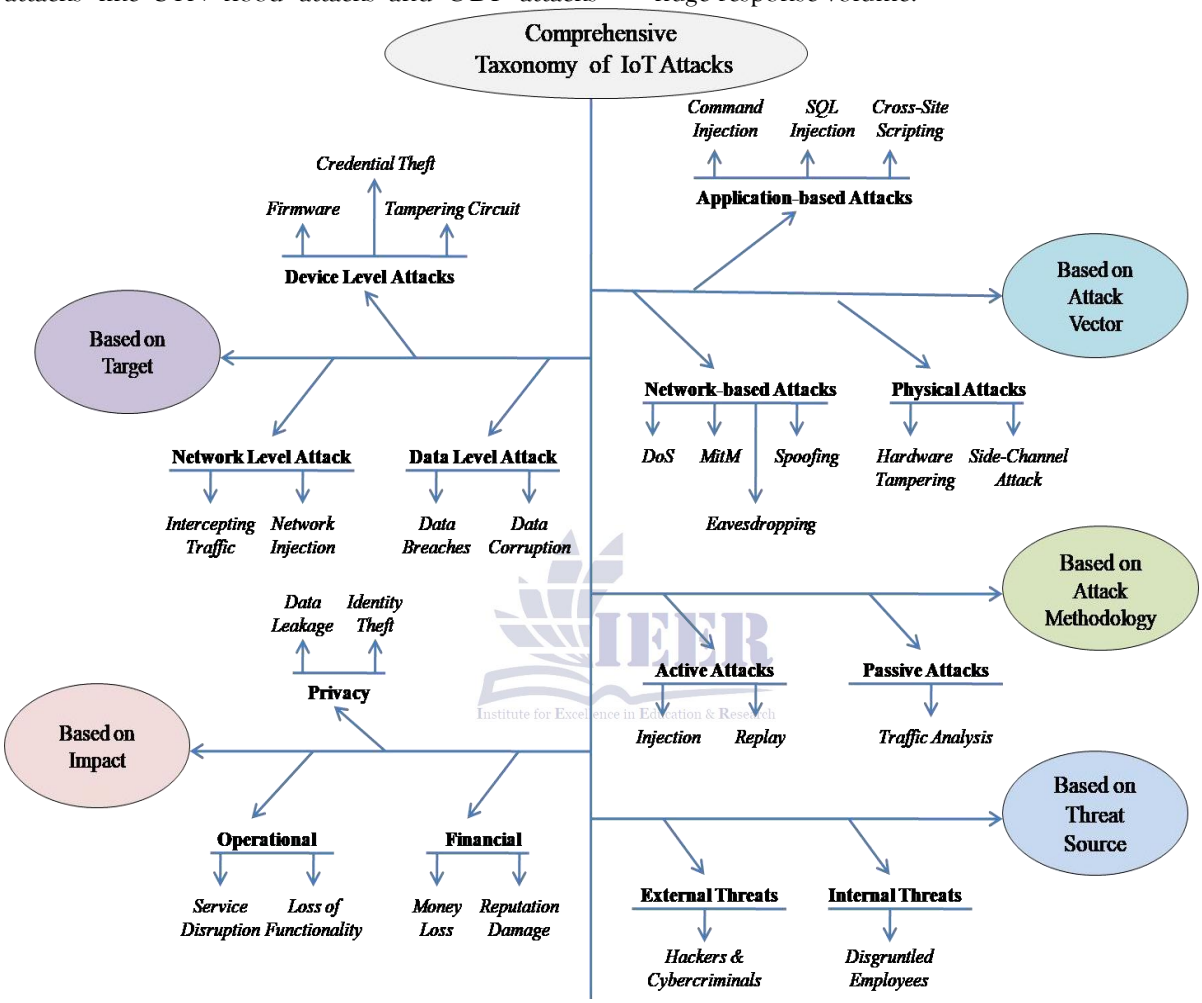

Figure 2: Attack Taxonomy in Internet of Things

Literature Survey: ***State-of-the-art Lightweight IDS***

In contrast to general-purpose computers, which typically have substantial storage and computational resources, IoT devices are generally constrained by limited storage and processing power. Although IDS solutions have been known to provide high security to traditional information technology nfrastructures, the resource constraint associated with IoT devices does not allow traditional IDS solutions to be used to provide security to IoT environments. The development of IDS solutions to provide security to IoT environments is a challenge to security due to the resource constraint associated with IoT devices.

Table 2: DDoS attacks and their impact on computing resources

Attack	CPU	Memory	Bandwidth	Protocol	Tools	Attack Volume	Duration
SYN Flood	High	Low	High	TCP	LOIC; Hping3; Metasploit	100s of Gbps	Min to Hours
UDP Flood	Low	Low	High	UDP	UDP Unicorn; LOIC; Metasploit	100s of Gbps	Min to Hours
HTTP Flood	Medium	Medium	High	HTTP	LOIC; HOIC; GoldenEye	10s to 100s of Gbps	Min to Hours
ICMP Flood	Low	Low	High	ICMP	Ping; LOIC; Metasploit	10s to 100s of Gbps	Min to Hours
DNS Amplification	Low	Low	Very High	UDP	Metasploit; LOIC; DNS scripts	100s of Gbps to Tbps	Min to Hours
NTP Amplification	Low	Low	Very High	UDP	Metasploit; LOIC; NTP scripts	100s of Gbps to Tbps	Min to Hours
Smurf Attack	Low	Low	High	ICMP	Smurf; LOIC	10s to 100s of Gbps	Min to Hours
Slowloris	Low	High	Low	HTTP	Slowloris; LOIC	–	Hours to Days
Reflected Amplification	Low	Low	Very High	Various	Metasploit; LOIC; Reflection script	100s of Gbps to Tbps	Min to Hours

Consequently, the main aim of the researchers is to develop light and efficient IDS solutions that can effectively secure IoT networks against any probable cyber attacks while optimizing the usage of the accessible resources. As in (Hai, Huh et al. 2010) assert, light-weight solutions are mostly developed with the aim of minimizing energy consumption as well as computational resources. As outlined in (Maleh and Ezzati 2015), a light-weight system can be described as one with low energy consumption. Thus, a lightweight system is typically characterized by its ability to perform necessary computations while using minimal resources.

Conversely, (Roesch 1999) defined lightweight IDS as a small module that needs only a small amount of memory, just enough so that it becomes a permanent resident in the Wireless Sensor Network (WSN) security architecture. Additionally, lightweight IDS was defined by (Othman, Madani et al. 2013) as a security system that requires a small amount of computational power, storage space, and energy while providing the required security.

Unlike other computers, which are normally equipped with large memory and processing capacities, most devices in IoT systems normally pose a challenge in terms of low memory and

processing capacities. Even though it can be very effective to apply IDS solutions in protecting computers from different kinds of cyber threats and attacks, it is impossible to apply IDS solutions in most devices in IoT systems because of low memory and processing capacities.

The major challenge that is likely to be encountered in the development of an IDS solution in the IoT environment is the increase in the requirements related to the capacity of the memory and the lifespan of the battery related to the IoT device. Therefore, researchers have continued to direct more emphasis in the development of an efficient solution to the problem related to the IDS solution in the IoT environment, which is considered to play a more significant role in the protection of the IoT environment against various types of cyber attacks. According to (Hai, Huh et al. 2010), the main aim associated with the development of a lightweight solution is to reduce the energy requirements to the minimum. According to (Maleh and Ezzati 2015), it is important to understand that a lightweight solution is deemed to have low energy requirements. In essence, it is important to understand that a lightweight solution can be defined as a solution that is capable of performing computations with the minimum resources. Lightweight IDS should be defined as a small module with minimal memory capacity at all times. The minimal memory capacity will be sufficient enough for a WLAN/WSN safety framework to be a constant addition at all times. Based on (Othman, Madani et al. 2013), lightweight IDS should be defined as a solution with minimal memory and/or energy capacity while still being able to satisfy the fundamental and principal needs in relation to safety objectives at all times

.Authors in (Fatima, Rehman et al. 2023) proposed an intrusion detection system suitable for an IoT platform with limited computational resources. In this system, authors used a chi-squared filter-based approach for selecting features in order to train ML classifiers such as RF, DT, SVM to classify network traffic as benign or malicious. Performance was measured using CPU, memory, FPR, TPR, and execution time for both training and testing. The experimental outcomes showed that, compared to other classifiers, RF performed better by achieving higher accuracy, lower resource consumption, reduced FPR, improved TPR, and reduced execution time.

In the study conducted by (Khanday, Fatima et al. 2023), the authors developed an approach in which the ExtraTreesClassifier and the Gini Impurity of the Random Forest classifier can be utilized in selecting the key features of the BOT-IoT and TON_IoT data sets. Subsequently, the ML classifiers can be utilized in training the selected key features of the data sets in developing an effective intrusion detection system in identifying the occurrence of DDoS attacks. However, the authors failed to report the CPU and memory. However, the authors did not report the CPU and memory usage of the proposed method.

A lightweight IDS using ML algorithms and focusing on improving FS using ridge regression-based techniques is proposed in (Azimjonov and Kim 2024). Various FS techniques are used in this work, and these are: using importance coefficient-based FS techniques, backward and forward selection techniques, and correlation coefficient-based FS techniques.

Heproposed workis implemented using KDD-CUP-1999, BotIoT-2018, andN-BaIoT-2021datasetsand elected twelve features. The

results show high accuracy in detecting network intrusion attacks.

Saheed et al. in (Saheed, Abiodun et al. 2022) proposed an ML-based intrusion detection system for the IoT network using the UNSW-NB15 dataset. In the proposed model, principal component analysis was used for feature reduction by selecting 10 features from the total of 44 to train the classifiers. Various ML algorithms such as XGBoost, CatBoost, KNN, SVM, QDA, and Naïve Bayes were used to train the models. In the proposed model, the accuracy of the classifiers was found to be more than 95%, whereas the training time was more for the CatBoost model. In contrast, the accuracy was also more for the proposed model using the SVM and KNN algorithms but with a lesser training time. Testing time, CPU usage, and memory usage were not considered in the proposed model.

Roy et al. (Roy, Li et al. 2022) proposed a B-Stacking feature selection enabled intrusion detection system for efficient use in the IoT network, which utilizes ensemble learning for accuracy. Boosting and stacking are used, with a level-0 learner to reduce bias, then a level-1 learner, and finally, parallel learning for efficient computation to optimize the model. Experiments conducted on NSL-KDD, KDD-CUP-1999, and CICIDS2017 datasets included preprocessing steps such as multicollinearity analysis, sampling, and reduction. The results obtained included lower CPU and RAM usage during the B-stacking stage, higher accuracy, and lower false alarm rates when compared to other methods. The datasets used were not specific to IoT devices. The cost of sampling and reduction was also not taken into consideration.

Sai et al. (Sai, Gupta et al. 2021) proposed a lightweight intrusion detection system based on a correlation-based feature selection strategy to identify features most relevant to the target variable. Using the UNSW-NB15 dataset, only three out of 44 features were selected and used to train a support vector machine classifier. The experimental results showed an accuracy of 98%; however, the study did not evaluate resource usage associated with the classifier's performance.

Ozer et al. in their study (Özer, Iskefiyeli et al. 2021), a lightweight model of detection of cyber attack based on four main Steps of Data Gathering, Cleaning, Modling, and Evaluation, Implemented in Real Time and Used for Evaluation of the Performance of a Classifier" by Özer, Iskefiyeli, et al. 2021, presented a model of a lightweight cyber-attack detection model, which is divided into four main steps of data gathering, data cleaning, modeling, and evaluation, implemented in real-time mode. As a part of this model, a permutation-based technique was presented, which helps in generating unique pairs of features, out of which the pair with maximum accuracy is selected. Moreover, the time complexity of the algorithm was also determined. Although high accuracy was reported by the application of the Random Forest, Decision Tree, Neural Network, and AdaBoost algorithms, these algorithms failed to maintain this accuracy in real-time mode. As a part of this model, 12 features were considered, out of which 10 features were selected.

Omar and George (Omar and George 2021), presented a study, an experimental setup including network consisting of various Wi-Fi security cameras installed indoors and outdoors to test the method for efficient cyber-attacks in an IoT network. To reduce the training time, optimize the model, and avoid overfitting, a correlation coefficient method for selecting the features of the model, which are relevant to the

input, was used to filter out the irrelevant input features to the model. Various ML algorithms, including SVM, DT, RF, LDA, SGD, and kNN, were
used to test the model, but the resources utilized by the model were not evaluated..

Khater et al. (Khater, Abdul Wahab et al. 2021), proposed a lightweight IDS for an IoT-based approach system. The steps of the proposed approach begin by exploring the given data, specifically the ADFA-LD dataset, to differentiate normal packets from attack packets, followed by feature extraction by utilizing an N-Gram transformation approach, feature selection by utilizing Mutual Information (MI) and PCA, followed by an MLP classification approach, where during testing, the performance of the MLP is validated by utilizing DT, RF, SVM, kNN, and NB classifiers, where it is clear that RF requires the minimum memory usage, followed by high accuracy and low FPR, thus confirming that MLP is not an appropriate approach for an IoT-based approach.

Lee et al. (Lee, Yoo et al. 2020) presented an optimized classification model, called IMPACT, or IMPersonation Attack DetecTION, in their article "IMPersonation Attack DetecTION: An Optimized Classification Model in Intrusion Detection Systems" authored by Lee, Yoo et al. in 2020. The system includes three major steps: feature extraction, feature selection, and classification. In feature extraction, the stacked autoencoder method, or SAC, using a deep neural network, reduces 154 features into 50 new features. In feature selection, 204 features are selected using the mutual information method and C4.8, and then five most dominant features are selected using an SVM classifier. Although it shows excellent results in terms of detection of both normal and attacking packets, it also shows higher rates of false alarm compared to other models.

The model for a misuse-based IDS was developed by Kumar et al. (Kumari and Jain 2023). The model was divided into two parts. The first was to develop an integrated rule-based IDS using the UNSW-NB15 dataset. The second was to develop a real-world dataset for testing its performance. The model was developed to improve its accuracy and minimize computational complexity by calculating information gain for selecting relevant attributes. The model selected 22 out of 47 relevant features for its development based on information gain calculated for each attribute. The model was developed using different decision tree models such as C5, CHAID, CART, and Quest algorithms. The highest accuracy obtained was 83.8%, but its effectiveness may be limited as it is a signature-based model.

Rani and Kaushal (Rani and Kaushal 2020) suggested a Network Intrusion Detection System (NIDS) with an implementation of RF classifiers for intrusion detection in IoT devices' networks. The proposed system was trained and validated using the KDD-CUP-1999 and NSL-KDD datasets. The training and validation time was minimized by choosing only 10 out of 41 features in the datasets with an accuracy of 99.9%. However, no information was offered regarding feature selection techniques utilized in their work.

The authors (Hikal and Elgayar 2020) proposed a framework for anomaly detection in IoT networks that involves three stages: Data Aggregation to collect data from IoT devices, Data Preprocessing to remove duplicate data and apply feature selection for dimension reduction, and MLIDS that uses SVM, RF, BPNN, DT to detect anomalies in network traffic. The authors used self-collected data to evaluate their proposed

system, where lightweight IDSs were found to obtain good accuracy with faster training/testing time. However, the authors failed to evaluate their system based on resource consumption.

A lightweight intrusion detection system known as Hawkware was introduced by Ahn et al. (Ahn, Yi et al. 2020) in their research article titled "Hawkware: A Lightweight Intrusion Detection System for Internet-of-Things Devices." This system comprises two parts, the monitor module, which analyzes the behavior of the network and devices to determine the key features, and the detection module, which processes the input to identify suspicious behavior associated with network intrusions. This system employs Network Behavior Feature Vectors extracted from the header of the packet and Device Behavior Feature Vectors obtained from the system calls to simplify the processing complexity. The training of the model was done offline, which may create a bias for the system in the field. The experiments for the research article used a Raspberry Pi with considerable processing power, which may be a problem for the system to be used with the IoT devices, which may lack processing power

Research study (Harriman, Serati et al. 2005) has suggested an efficient intrusion detection system using fuzzy logic for protecting MQTT IoT networks from DoS attacks on IoT devices. This IDS system has been primarily developed for the following purposes: detection of DoS attack, efficiency, and quick detection of the attack. In the IDS system, fuzzy logic has been employed to detect the attack by using the Connection Message Ratio (CMR) and Connection Acknowledgment Message Ratio (CAMR) values to mark the attack as "safe" or "malicious." Important features have been extracted from trace data, although it is unclear what FS method was used in this research study for selecting important features.

The IDS proposed (Bakhtiar, Pramukantoro et al. 2019) is used to detect DoS attack using J48 classification algorithm. The IDS was trained on a dataset created from a real network environment using Information Gain to obtain the most important features from the dataset. The IDS was effective when it was trained on a chosen number of 20 features from 100 features.

Authors in (Jan, Ahmed et al. 2019) proposed a light-weight attack detection system utilizing an SVM classifier for detecting nodes transmitting anomalous data in IoT network flows. The system utilized a single feature, namely the packet arrival rate per node, thereby reducing complexity and being efficient in DDoS attack classification, although it faced difficulties in concurrent action detection due to the utilization of a single feature.

Soe et al. (2020) introduced another lightweight anomaly detection system for IoT networks employing correlation-based feature selection to choose the top seven features from 49. These features were used to train a J48 classifier, and testing achieved an average detection rate of 99% across all attack types. Table 3 presents the studies proposed a feature selection based lightweight intrusion detection systems for resource-limited IoT. Because of the reduced processing capabilities found on IoT devices, the need for designing efficient and resource efficient solutions for IDS cannot be overemphasized. As previously discussed, an anomaly-driven IDS is built with ML methodologies, yet these designs consume high resources for effective operation.Consequently, the strategy followed by researchers designing such IoT solutions has incorporated FS techniques into their designs.

Table 3: *Review of state-of-the-art studies for lightweight ID*

Paper	Dataset	ML Algorithm	Accuracy	Approach	System Specs	Time (ms)	Memory	CPU	Test Time	Train Time
(Khanday, Fatima et al. 2023)	TON_IoT &BOT-IoT	NB, SVM, LR, ANN, LSTM	99%	Feature Selection	--	--	--	--	--	--
(Azimjono and Kim 2024)	KDD-CUP-v1999, BOT-IoT & NBaIoT-2021	Stochastic Gradient Descent	94%	Feature Selection	--	2.545	29.812	--	--	--
(Saheed, Abiodun et al. 2022)	NSL-KDD, CICIDS2017	B-Stacking classifiers	98.50%	Feature Selection	8GB, 2.9GHz	202	80	--	--	--
(Sai, Gupta et al. 2021)	UNSW-NB15	SVM	98%	Feature Selection	--	--	--	--	--	--
(Özer, Iskefiyeli et al. 2021)	BoT-IoT	KNN, SVM, DT, RF, NN, NB, QDA	90%	Feature Selection	--	426	--	--	--	--
(Omar and George 2021)	IoTID20	SVM, KNN, MLP, DT, RF, LDA	98%	Feature Selection	4GB	--	80	--	--	--
(Khater, Abdul Wahab et al. 2021)	ADFA-LD	MLP	96%	Feature Selection	4.4GHz	4.4	4	--	--	--
(Rani and Kaushal 2020)	NSL-KDD, KDD-CUP-1999	RF	99.90%	Feature Selection	--	1.78	0.28	--	--	--
(Lee, Yoo et al. 2020)	AWID	SVM	98.22%	Feature Selection	--	299.97	--	--	--	--
(Khater, Abdul Wahab et al. 2021)	-	DT	83%	Feature Selection	--	--	--	--	--	--
(Hikal and Elgayar 2020)	Self-generated	RF, DT, SVM, BPNN	99.70%	Feature Selection	--	30000	113000	--	--	--
(Ahn, Yi et al. 2020)	Self-generated	ANN	99.90%	Feature Selection	--	1.7	2.7	--	--	--
(Azimjono and Kim	v-	Fuzzy logic	80%	Feature Selection	--	--	--	--	--	--

2024)											
(Bakhtiar, Pramukant et al. 2019)	Self-generated oro	J48	100%	Feature Selection	128GB, 2.6GHz	0.035	12.28	13	~	~

2. Research Gaps and Emerging Challenges in DoS/DDoS Attack Detection for Resource Constrained IoT Devices

This section should contain each and every detail pertaining to methods and materials used in the experiments. The section can be sub-divided in sub-headings i.e. study site, sampling protocole, statistical analysis etc.

- ***Limitations with filter-based FS in designing lightweight IDS:*** From the literature review covered under section 2.7, it is clear that FS is found to have been used widely in the design of lightweight intrusion detection systems for resource-constrained IoT devices. FS using filters is widely used for selecting highly correlated features from a pool of available features in a dataset for classification tasks. Meanwhile, filter-based FS is also known for efficiency gains in lowering both training time as well as test time with reduced resource cost. However, using FS with filter-based techniques as a stand-alone technique might limit adaptability and efficiency of performance of the IDS model since filter-based FS requires pre-defined statistical thresholds to evaluate feature relevance. Although using statistical thresholds for FS might result in efficiency gains for faster FS, statistical thresholds might not capture subtle underlying patterns adequately to avoid feature exclusion with potential relevance to address specific attack detection needs for more generalizable outcomes.
- Recent DoS/DDoS attacks

The discussion shown in recent DoS/DDoS discussion clearly explains how DoS/DDoS attacks affect the services provided for lawful users. However, due to the complexities involved with current DoS/DDoS attacks, it is clear that current security measures lack efficacy in detecting these attacks. Specifically, the current methods may lack effectiveness, especially in detecting advanced attack methods like zero-day attacks, which usually exploit unknown vulnerabilities. Hence, the development of more effective security measures is necessary to facilitate the detection of advanced DoS/DDoS attack methods.

- IDS gap adaptive approach for detection of new attacks

The process design for IDS that uses ML algorithms mandates intensive resource support for accommodating training and testing processes. In the context of securing resource-constrained IoT environments against constantly emerging threats, an integral need exists for adaptive security solutions that are resource-effective and efficient. These solutions should be able to adapt dynamically to emerging threats.

- Resource Efficient Self-healing Approach

IoT networks require IDS capable of dynamically adapting to emerging threats while remaining lightweight. Many ML-based IDS solutions are static and require high computational resources for retraining.

3. Conclusion

This paper presents a detailed overview of resource-limited IoT devices and the attack taxonomy in

IoT-based systems, and also discusses the impact of DoS/DDoS attacks on computing resources, showing that IoT devices with limited computing power are highly vulnerable to these attacks. This paper also presents a comprehensive survey of state-of-the-art existing IDS proposed for resource-constrained IoT devices against DoS/DDoS attacks. We found that feature selection approach is one of the most prominent technique to design lightweight IDS. We have also provided the detailed insights into the strength and limitations of existing studies and providing the future research perspectives to design more robust and efficient IDS solutions consider resource constrained nature of IoT.

Acknowledgment

We express our heartfelt gratitude to the researchers for contributing their valuable insights to enhance the study.

Conflict of Interest

Authors have no conflict of interest

Funding (if any)

No funding received for this study.

Author contribution

Mahawish Fatima: Writing – original draft, Methodology, Investigation, Conceptualization. **Osama Rehman**: Writing – review & editing, Supervision. **M. Hassan Nasir:** Writing – review & editing, Methodology, Conceptualization. **M.Ashraf:** Writing – review & editing. **Hina Shakir:** Writing – review & editing. **Muahmmad Hussain:** Writing – review & editing. **Bushra Fazal Khan:** Writing – review & editing.

References

Ahn, S., et al. (2020). Hawkware: Network intrusion detection based on behavior analysis with ANNs on an IoT device. 2020 57th ACM/IEEE Design Automation Conference (DAC), IEEE.

Alamiedy, T. A., et al. (2018). Review on feature selection algorithms for anomaly-based intrusion detection system. International Conference of Reliable Information and Communication Technology, Springer.

Aminu Ghali, A., et al. (2020). Comparative analysis of DoS and DDoS attacks in Internet of Things environment. Computer Science On-Line Conference, Springer.

Azimjonov, J. and T. Kim (2024). "Designing accurate lightweight intrusion detection systems for IoT networks using fine-tuned linear SVM and feature selectors." Computers & Security 137: 103598.

Bakhtiar, F. A., et al. (2019). A lightweight IDS based on j48 algorithm for detecting DoS attacks on IoT middleware. 2019 IEEE 1st global conference on life sciences and technologies (LifeTech), IEEE.

Cai, J., et al. (2018). "Feature selection in machine learning: A new perspective." Neurocomputing 300: 70-79.

Chen, C. W., et al. (2020). "Ensemble feature selection in medical datasets: Combining filter, wrapper, and embedded feature selection results." expert systems 37(5): e12553.

Damon, E., et al. (2012). Hands-on denial of service lab exercises using slowloris and rudy. proceedings of the 2012 information security curriculum development conference.

Fatima, M., et al. (2023). Li-ids: An approach towards a lightweight ids for resource-constrained iot. 2023 International Conference on Smart Applications, Communications and Networking (SmartNets), IEEE.

Fatima, M., et al. (2024). "ELIDS: ensemble feature selection for lightweight IDS against DDoS attacks in resource-constrained IoT

environment." Future Generation Computer Systems 159: 172-187.

Fatima, M., et al. (2024). Ensemble Feature Selection based Lightweight IDS Tailored for DDoS Attacks Detection over IoT Devices. 2024 International Visualization, Informatics and Technology Conference (IVIT), IEEE.

Hai, T. H., et al. (2010). "A lightweight intrusion detection framework for wireless sensor networks." Wireless Communications and mobile computing 10(4): 559-572.

Harriman, J., et al. (2005). Comparison of transmissive and reflective spatial light modulators for optical manipulation applications. Optical Trapping and Optical Micromanipulation II, SPIE.

Hikal, N. A. and M. Elgayar (2020). Enhancing IoT botnets attack detection using machine learning-IDS and ensemble data preprocessing technique. Internet of Things—Applications and Future: Proceedings of ITAF 2019, Springer: 89-102.

Humayun, M., et al. (2024). "Securing the Internet of Things in artificial intelligence era: A comprehensive survey." IEEE Access 12: 25469-25490.

Impersonation attack detection via edge computing using deep autoencoder and feature abstraction." IEEE Access 8: 65520-

Jan, S. U., et al. (2019). "Toward a lightweight intrusion detection system for the internet of things." IEEE Access 7: 42450-42471.

Jordan, M. I. and T. M. Mitchell (2015). "Machine learning: Trends, perspectives, and prospects." Science 349(6245): 255-260.

Joshi, A. V. (2020). "Machine learning and artificial intelligence."

Junejo, K. N. and J. Goh (2016). Behaviour-based attack detection and classification in cyber physical systems using machine learning. Proceedings of the 2nd ACM international workshop on cyber-physical system security.

Khader, R. and D. Eleyan (2021). "Survey of dos/ddos attacks in iot." Sustainable Engineering and Innovation 3(1): 23.

Khan, M. M., et al. (2009). "High error-rate quantum key distribution for long-distance communication." New Journal of Physics 11(6): 063043.

Khanday, S. A., et al. (2023). "Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks." Expert Systems with Applications 215: 119330.

Khater, B. S., et al. (2021). "Classifier performance evaluation for lightweight IDS using fog computing in IoT security." Electronics 10(14): 1633.

Kumari, P. and A. K. Jain (2023). "A comprehensive study of DDoS attacks over IoT network and their countermeasures." Computers & Security 127: 103096.

Lavrenovs, A. (2023). "MEASURING DISTRIBUTED REFLECTED DENIAL-OF-SERVICE AMPLIFIED VOLUMETRIC

Lee, S. J., et al. (2020). "IMPACT:

Maleh, Y. and A. Ezzati (2015). "Lightweight Intrusion Detection Scheme for Wireless Sensor Networks." IAENG International Journal of Computer Science 42(4).

Moore, S. J., et al. (2020). "IoT reliability: a review leading to 5 key research directions." CCF Transactions on Pervasive Computing and Interaction 2(3): 147-163.

Mrabet, H., et al. (2020). "A survey of IoT security based on a layered architecture of sensing and data analysis." Sensors 20(13): 3625.

Mukhopadhyay, S. C. and N. K. Suryadevara (2014). "Internet of things: Challenges and

opportunities." Internet of things: Challenges and opportunities: 1-17.

Nasir, H., et al. (2019). "Intrusion Detection: Tools, Techniques and Trends." Sindh University Research Journal-SURJ (Science Series) 51(2).

Nayak, G., et al. (2022). "Depth analysis on DoS & DDoS attacks." Wireless Communication Security: 159-182.

Ojo, M. O., et al. (2018). "A review of low-end, middle-end, and high-end iot devices." IEEE Access 6: 70528-70554.

Omar, M. and L. George (2021). Toward a lightweight machine learning based solution against cyber-intrusions for IoT. 2021 IEEE 46th Conference on Local Computer Networks (LCN), IEEE.

Othman, M., et al. (2013). "A survey of mobile cloud computing application models." IEEE communications surveys & tutorials 16(1): 393-413.

Özer, E., et al. (2021). "Toward lightweight intrusion detection systems using the optimal

Pal, M. and G. M. Foody (2010). "Feature selection for classification of hyperspectral data by SVM." IEEE Transactions on Geoscience and Remote Sensing 48(5): 2297-

Rani, D. and N. C. Kaushal (2020). Supervised machine learning based network intrusion detection system for Internet of Things. 2020 11th International conference on computing, communication and networking technologies (ICCCNT), IEEE.

Roesch, M. (1999). Snort: Lightweight intrusion detection for networks. Lisa.

Rose, K., et al. (2015). "The internet of things: An overview." The internet society (ISOC) 80(15): 1-53.

Roy, S., et al. (2022). "A lightweight supervised intrusion detection mechanism for IoT networks." Future Generation Computer Systems 127: 276-285.

Saheed, Y. K., et al. (2022). "A machine learning-based intrusion detection for detecting internet of things network attacks." Alexandria Engineering Journal 61(12): 9395-

Sai, K. M., et al. (2021). Lightweight Intrusion Detection System In IoT Networks Using Raspberry pi 3b+. SysCom.

Salim, M. M., et al. (2020). "Distributed denial of service attacks and its defenses in IoT: A survey." Journal of Supercomputing 76(7).

Scheuer, S., et al. (2011). "Exploring multicriteria flood vulnerability by integrating economic, social and ecological dimensions of flood risk and coping capacity: from a starting point view towards an end point view of vulnerability." Natural hazards 58(2): 731-

Sharif, D. M., et al. (2023). "Detection of application-layer DDoS attacks produced by various freely accessible toolkits using machine learning." IEEE Access 11: 51810-

Turgunbaev, R. (2024). "Machine Learning and Its Use in the Automatic Extraction of Metadata from Academic Articles."

Velan, P., et al. (2015). "A survey of methods for encrypted traffic classification and analysis." International Journal of Network Management 25(5): 355-374.

Wang, H., et al. (2002). Detecting SYN flooding attacks. Proceedings. Twenty-first annual joint conference of the IEEE computer and communications societies, IEEE.

Yoshiyama, M., et al. (1995). "Interfacial morphology and strength of bonds made to superficial versus deep dentin." American journal of dentistry 8(6): 297-302.