

# DDoS Cyberattacks in Smart Home IoT Networks and Common Mitigation Techniques

Oghenetejiri Okporokpo<sup>1</sup>, Funminiyi Olajide<sup>2</sup>, Nemitari Ajienka<sup>3</sup> and Xiaoqi Ma<sup>4</sup>

<sup>1</sup> Department of Computer Science, Nottingham Trent University, Clifton Lane, Nottingham  
NG11 8NS

oghenetejiri.okporokpo2022@my.ntu.ac.uk

funminiyi.olajide@ntu.ac.uk

nemitari.ajienka@ntu.ac.uk

xiaoqi.ma@ntu.ac.uk

**Abstract.** The prevalence of smart home Internet of Things (IoT) devices has led to an increased adoption worldwide. The widespread acceptance and adoption of these smart home devices by both organizations and individuals can be attributed to the numerous advantages facilitated by the advancing Internet of Things (IoT) technologies. These technologies incorporate sensors, cameras, and actuators in devices, enabling them to gather information from the surroundings and perform designated tasks, thereby simplifying users' daily lives and work. However, the emergence of various types of smart home devices has significantly amplified the cyber threat landscape and subsequently this has resulted in a heightened demand for enhanced cybersecurity measures. The escalation and evolution of digital threats targeting smart home networks have led to several innovations. However, despite extensive research and investigations, Distributed Denial of Service (DDoS) attacks remain a pervasive and common attack vector targeting smart home IoT networks. This study delves into various existing DDoS attack types targeting smart home IoT networks and the common cybersecurity approaches tailored for mitigating these unique challenges. Additionally, we classified the mitigation techniques into three major categories, namely: Action or Event-based, Location-based & Hybrid-based systems. Finally, the challenges associated with each of these techniques we highlighted and future research directions in this emerging field presented.

**Keywords:** DDoS, Cyberattack, Security, Privacy, Intrusion & Detection.

## 1 Introduction

As the world becomes more dependent on Internet of Things (IoT) devices and their interconnections for technological development, the need for better security has also increased. Cybercrime and other digital threats are on the increase at a rate directly proportional to the rate of increase in the dependence on the use of smart home devices [1]. Smart home Internet of Things (SHIoT) networks comprise an interconnected environment, where diverse electronic devices and appliances

collaborate to offer intelligent services seamlessly to individuals [2]. SHIoT represents the convergence of various technologies interlinked to deliver innovative services. Key features of smart homes include real-time event monitoring, remote control capabilities, intruder detection, and safety measures such as gas and fire alarms. Given the management of sensitive and personal data within smart homes, it is imperative to implement robust security and privacy solutions. This ensures the safeguarding of corporate and personal data against potential exploitation while simultaneously ensuring the seamless delivery of reliable services [3].

Smart home IoT networks are known to be susceptible to a wide range of cyberattack vectors including DDoS attacks, Man-in-the-middle attacks (MITM), brute-forcing, eavesdropping, privilege scaling to more sophisticated ransomware attacks, and many more [4]. In May 2023, the US Federal Trade Commission (FTC) charged home security camera company Ring with compromising its customers' privacy by lapses in securing customer data and by failing to implement basic privacy and security measures which enabled cyber attackers to take control of consumers' accounts, cameras, and videos. More than 55,000 Ring customers suffered from multiple credential stuffing and brute force attacks, resulting in refunds totalling more than \$5.6 million to US consumers because of the settlement [5].

The security of IoT devices has been studied by several researchers. A new DDoS detection and DDoS mitigation architecture was proposed by Mihoub, Alaeddine, et al. [6]. The proposed architecture provides fine-granularity detection, by identifying the nature of the cyberattack as well as the means of attack propagation. Then finally apply the corresponding mitigation countermeasure based on the prediction attack result. Researchers Paudel et al. investigated the use of a Graph-based Outlier Detection approach as a means of securing IoT network traffic as a real-time graph stream. The study scrutinized the security of applications developed based on the IoT traffic dataset generated from real-life IoT environments created with 28 different IoT devices [7]. Other studies highlight cybersecurity challenges in IoT network environments, including unauthorized insecure communications [8], eavesdropping [9], packet sniffing attacks [10], Encryption attacks [11], Ransomware attacks [12], and malicious code [13].

A vulnerability assessment of SHIoT devices conducted by Pooja, et al. [14] reveals numerous vulnerabilities and associated threats that could compromise user privacy, user data, traffic content, and lead to resource access disruption through Denial of Service (DoS) attacks. The abundance of network and data resources in a smart home environment poses a significant security challenge, often exacerbated by DoS attacks. Smart home devices have often been the core vehicle through which DoS attacks are launched but they also face the risk of being the targets of various forms of DoS attacks [15]. The rise in the number of such devices raises concerns about the potential escalation of more frequent and intense attacks in the future. Despite this, there is a paucity of research addressing this issue.

Our research builds upon previous literature reviews on cyberattacks and the security of smart homes. This research aims to identify the various existing DDoS

attack vectors targeting smart home IoT networks and the common cybersecurity approaches tailored for mitigating these unique challenges. Additionally, the research aims to classify the identified DoS cyberattacks by taxonomy. The research results will establish a robust foundation for further studies, contributing to the development of a detection and management model for DDoS traffic both emanating from and targeting Smart Home Internet of Things (SHIoT) network environments. The main contributions of this research are outlined as follows:

- We present a comprehensive classification of the current DDoS attacks in IoT based on the reviewed literature.
- We identify the existing DDoS mitigation techniques deployed in securing SHIoT networks.
- A detailed analysis of DDoS detection and mitigation techniques identified are presented in this paper. Also, based on the reviewed literature, these techniques are grouped into 3 major categories, namely: Action or Event-based, Location-based & Hybrid-based systems. The challenges associated with each of these techniques are also highlighted in this paper.

## 2 Related Work

As a crucial element within the IoT paradigm, smart home devices have efficiently catered to the needs of both individuals and industries by establishing communication with a diverse range of digital devices under the IoT framework. In an envisioned wired future, seamless communication among all devices within smart homes is the ideal scenario. IoT-driven smart home technology has significantly transformed human life, ensuring connectivity for virtually everyone irrespective of time and location [16]. However, the widespread connectivity, while simplifying and automating daily tasks, introduces security vulnerabilities. The vulnerability of IoT devices stems from a variety of reasons which include a lack of regular updates by manufacturers, the ubiquitous nature of IoT devices in terms of connectivity, and availability, coupled with the substantial amount of data exchange involved, as well as their limited computing power, constrained resources (space, battery, memory and bandwidth) [17].

Cybersecurity of IoT networks has consistently been known to be an interesting area for research and development. As IoT technology evolves, new threats and vulnerabilities continue to emerge. Several reviews have proposed methods to deal with the security challenges common with IoT networks [18]-[20]. The cybersecurity risks reviewed, and the techniques deployed by researchers vary with each focusing on multiple aspects of the security IoT networks by using an assortment of approaches.

The focus of this research is to identify the evolving DDoS cyber threats targeting SHIoT networks and devices as well as the common mitigation techniques available for detecting and dealing with these attacks when they occur. Table 1 below shows

other related works and how they differ from our research. The columns indicate the key contributions of our research work. A value of X indicates that the corresponding category (shown in the column) has not been dealt with by the related study (shown in the row), while ✓ indicates that the category has been addressed. The last row refers to our research.

**Table 1.** Comparison of other related studies of DoS/DDoS and SHIoT Cybersecurity.

| Reference       | Topic                                                | Publication Year | Specific to Smart Home Networks | Specific to DoS/DDoS Attacks | Classification |
|-----------------|------------------------------------------------------|------------------|---------------------------------|------------------------------|----------------|
| [17]            | Cybersecurity IoT Sensors                            | 2020             | ✓                               | ✓                            | X              |
| [21]            | Cybersecurity Smart Home                             | 2020             | ✓                               | X                            | X              |
| [22]            | Cybersecurity Smart Home                             | 2020             | ✓                               | X                            | X              |
| [23]            | Wireless Sensor networks                             | 2020             | X                               | X                            | X              |
| [24]            | Cybersecurity Smart Home IoT layers                  | 2021             | ✓                               | X                            | X              |
| [25]            | Smart Home Personal Assistants                       | 2021             | ✓                               | X                            | X              |
| [26]            | Digital harm of Smart Home IoT                       | 2023             | ✓                               | X                            | ✓              |
| [27]            | Cybersecurity of IoT                                 | 2023             | ✓                               | X                            | ✓              |
| [28]            | Privacy and Security of Smart Homes                  | 2024             | ✓                               | X                            | ✓              |
| [29]            | Cybersecurity of SDN-IoT                             | 2024             | X                               | X                            | ✓              |
| <b>Our Work</b> | <b>DoS/DDoS attacks Smart Home Networks/Devices.</b> | <b>NA</b>        | <b>✓</b>                        | <b>✓</b>                     | <b>✓</b>       |

**Legend - ✓-Yes, x-No**

Ladislav et al. [17] in their study, investigated the resistance of IoT Sensor devices against DDoS attacks. The research focused on examining how IoT sensor devices and networks react whilst under a DDoS attack. A case study was carried out using an Ansible real-time attack simulation Testbed environment. Three different test scenarios were considered, with a DDoS attack targeted at the sensor gateway with the network traffic being generated from a mobile application of the gateway manufacturer or a mobile application of the smart home personal assistant system and a third scenario involving traffic from a smart home personal assistant system. However, the scope of the research was very limited, with a narrow focus on specific attack vectors and traffic sources, and they failed to identify any mitigation strategies.

Researchers Davis et al. [21] conducted studies on the vulnerabilities and security posture of smart home IoT devices. The research included a review of documented vulnerability case studies related to IoT devices, covering four attack categories: physical, network, software, and encryption. Subsequently, vulnerability experiments were carried out, comparing the security postures of popular and unpopular vendors through misuse and abuse case analyses. Additionally, scrutiny of coverage in major vulnerability databases was undertaken. While the categorization of attacks was thorough, the depth of analysis within each category lacked detailed technical breakdowns of specific vulnerabilities and how they are exploited by attackers.

A study by Andrade et al. [22] explored the cybersecurity characteristics that outline an evaluation system of cybersecurity maturity of IoT solutions used for the development of smart city applications. A review based on a top-down approach to cybersecurity incident response in IoT ecosystems was carried out. Finally, a model based on risk levels was proposed to evaluate the IoT cybersecurity maturity in a smart city network environment. Although the study outlined a risk-level-based evaluation model, it lacked sufficient detail on the criteria and metrics used to define and measure the identified risk levels, which could result in inconsistencies in its application and potential challenges in achieving accurate assessments of cybersecurity. Pirbhulal, et al. [23] proposed a Triangle Based Security Algorithm (TBSA) for WSNs which backward integration to IoT-based smart home network environments. The mechanism deploys low-power nodes for the implementation of security during data transmission. The authors, however, did not adequately address the scalability of the algorithm, to evaluate how the TBSA performs as the number of nodes increases or in more complex network topologies typical of larger smart home environments.

Researchers, Touqeer et al. [24] carried out a survey of the most common security threats and privacy challenges affecting IoT networks and devices. The identified threats were categorized in a layered architecture of the IoT network environment. The main contribution of the survey was a review of cybersecurity challenges targeting the four-layer architecture of IoT networks. However, the study provided an overview rather than an in-depth examination of how the identified threats exploit specific vulnerabilities, as well as their impact. An evaluation of how users can leverage the use of Speech Processing Algorithms (SPA) to interact with IoT systems was done by researcher Obaid [25]. Subsequently, the article addressed system-related challenges and proposed solutions to enhance the technology's adaptability and versatility for easy integration with other related technologies. However, the author failed to differentiate between the unique challenges faced in various IoT environments such as smart homes, industrial IoT, and healthcare IoT, leading to a potentially oversimplified view of the vulnerabilities.

Aldahmani et al. [27] examined the cybersecurity challenges of IoT sensor devices by reviewing IoT design, objects, and standards which affect security and privacy. The researchers also introduced a taxonomy related to vulnerabilities, threats, and

attacks on IoT devices. Also, researchers Araya and Helena [30] reviewed anomaly-based cyberattack detection systems on intelligent home network environments, presented an adapted taxonomy to help classify existing anomaly detection methods and performed an analysis of the current state of knowledge in detection and placement, and validation strategies. However, the relevance of their taxonomy and observations was not substantiated by concrete evidence.

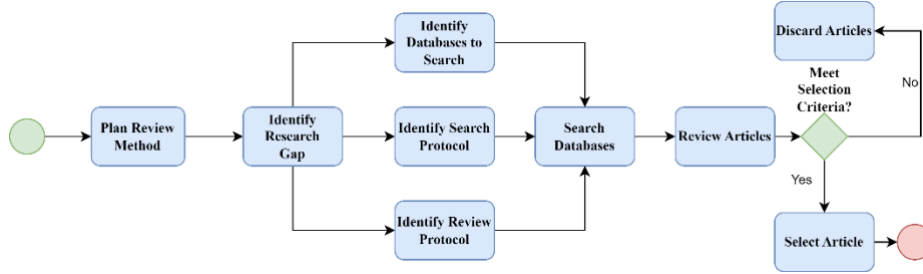
In the research by Buil-Gil et al., [26] the authors classified the digital harms of smart homes, identified smart home devices and potential features of the devices which make them attractive tools for digital harms and explored some approaches to mitigate the identified digital harms of smart homes. However, there were no specific examples of the results of the identified attacks to add depth and contextualize the highlighted techniques and classifications.

Magar and Zhou [28] conducted an examination of major IoT applications, including related security and privacy challenges. The researchers mainly identified security techniques deployed within smart homes and how to further enhance them. A taxonomy of common privacy, security, and integration issues within the context of the IoT layered architecture was presented. Finally, current research initiatives dedicated to the development of energy-efficient devices to aid in addressing some of the highlighted challenges in the IoT landscape were outlined. However, there was a lack of detailed information on the criteria for selection, data sources, and analytical methods used in the study. Singh and Jain [29] outlined the prevalent relationship between Software-defined networking (SDN) and IoT. The research mainly focused on identifying various types of DDoS attacks and different types of cyberattack detection, and mitigation methods employed to address DDoS threats within SDN-based IoT (SDN-IoT) networks.

There are several DDoS mitigation techniques [31], and there are numerous smart home IoT cybersecurity approaches, however, there appears to be a lack of a comprehensive classification system that categorizes these techniques based on their operational principles and effectiveness. To address the identified gap, a classification system categorizing DDoS mitigation techniques has been proposed. Techniques have been grouped into relevant categories, providing a clearer understanding of their application and effectiveness. This classification aims to enhance the implementation of DDoS mitigation techniques, ensuring a more structured and efficient approach to securing smart home IoT networks.

### 3 Methodology

A review process was carried out with the aim of surveying the existing knowledge about the topic of this research. The review methodology employed in this study is depicted in Figure 1. A comprehensive search strategy was implemented, involving distinct combinations of keywords across the specified databases.



**Fig. 1.** Primary Studies Selection Process.

The objective of this research was to identify the evolving DoS/DDoS cyber threats and common mitigation techniques in smart home IoT networks. Based on this objective, the following questions were put forward to guide the investigation:

- Which of the evolving DDoS cyberattacks are affecting Smart Home IoT networks (SHIoT)?
- What are the common DDoS mitigation techniques deployed in smart home IoT networks?

The following academic databases were used for this literature review:

SCOPUS, Web of Science, IEEE Xplore, Springer. Google Scholar was used as an initial source for general reading material.

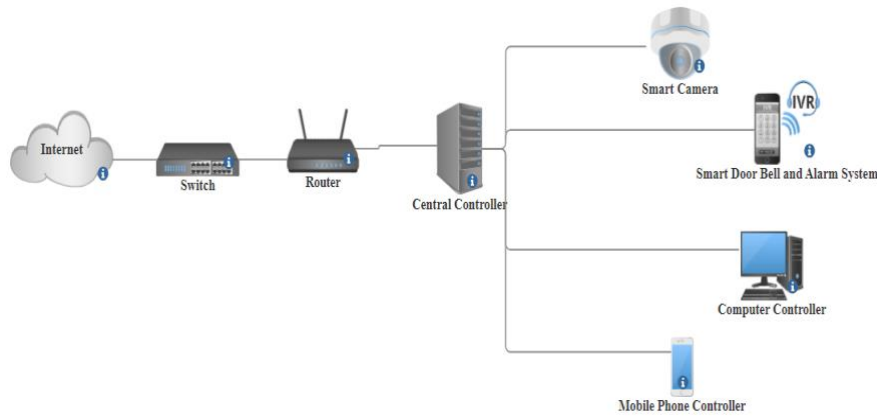
The specific keywords used in searching the databases include: “Smart Home”, “DoS”, “DDoS”, “Denial of Service”, “IoT” and “Cybersecurity”. Any article which contained the search terms or combinations of them was initially gathered. A total of 1,235 articles underwent initial review. To improve the quality of the results, filters we applied to the selected databases. The subject area was constrained to Computer Science and Computer Engineering, and the content type was restricted to Research Articles and Review Articles. Additionally, in Google Scholar, only review articles were selected. Duplicates were systematically removed, forward and backward snowballing identified an additional number of papers respectively, leaving a final count of 10 papers that were deemed valuable and accepted.

## 4 Smart Home Network Overview

The popularity of IoT smart home services is on the rise as devices efficiently communicate through Internet Protocol (IP) addresses. The smart home market is experiencing rapid growth, with the entry of major players in consumer electronics like Samsung and LG, along with IT companies like Google joining the flourishing market. These companies have introduced products and services that have the potential to significantly expand the smart home industry [32].

In a smart home environment, all devices are interconnected via the internet. However, with the increasing number of devices, so also does the risk of cyberattacks. Operating smart home devices independently can mitigate the likelihood of such attacks. Currently, smart home devices are accessible via the internet from anywhere, at any time, further elevating the potential for malicious exploits [18].

A smart home comprises four key components: the service platform, smart devices, home gateway, and home network. The service platform environment is comprised of, the home network, the home gateway and the smart devices. Within the smart home ecosystem, devices are interconnected and share information intelligently through the home network. To regulate the information flow among smart devices connected to the external network, a home gateway or central controller is in place. The service platform leverages the services of a service provider, delivering various services to the home network [33]. Figure 2. below is an example of a smart home network.



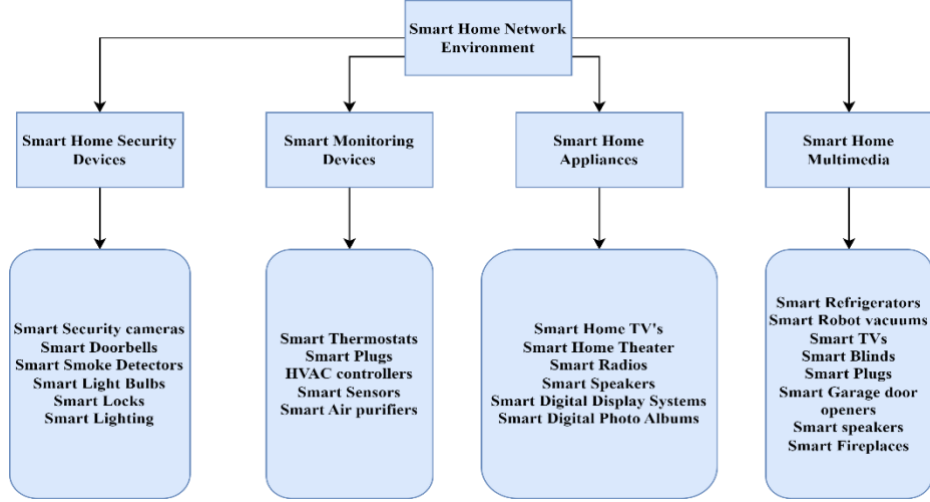
**Fig. 2.** Sample Smart Home Network Setup.

The prevalence of IoT smart home services is on the rise as digital devices effectively communicate through Internet Protocol (IP) addresses. The smart home market is experiencing rapid growth, with the entry of major players in consumer electronics like Samsung and LG, along with IT companies like Google joining the flourishing market. These companies have introduced products and services that have the potential to significantly expand the smart home industry [32].

#### 4.1 Classification of SHIoT

Apart from energy monitoring and control devices, other devices like motion sensors and temperature sensors can be integrated into the smart home network infrastructure thus forming part of the Smart Home Network Grid. There is a vast array of smart home devices including Security Devices, Monitoring Devices, Home Appliances and

Home Multimedia. Figure 3. below shows a depiction of the various categories of SHIoT devices.



**Fig. 3.** Smart Home Network Devices.

Furthermore, based on the smart home network environment management type, IoT devices can be classified as either locally managed or remotely managed devices, where remote-controlled devices are connected to the Internet, while locally managed devices are limited to the local area network they are connected to [34]. Generally, smart home network classifications encompass smart home devices, central network controllers as well as network communication traffic.

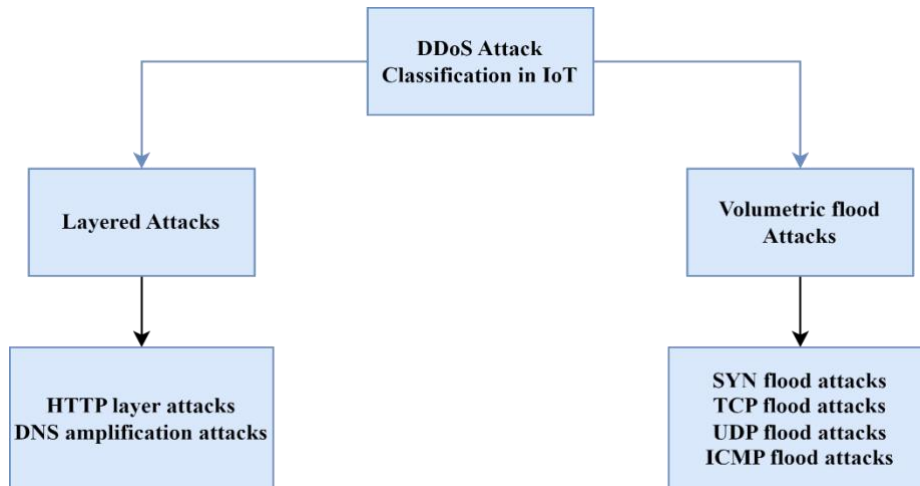
## 5 Attack Classification and Mitigation Techniques

Over the last few years, smart home devices have become more popular for personal use. With the ever-increasing penetration of internet access worldwide, and with a global internet user base of over five billion people, the number of smart home devices is on the increase. The use of smart devices for online business transactions has stood out as one of the emerging modern trends. Consumers are constantly adopting new smart home devices, with most devices being designed to have a one-click purchasing system to enable automated purchases and replenishment [35]. As the adoption of smart home devices continues to rise in popularity since the Covid-19 pandemic in 2020, it is estimated that cyberattacks have increased by over 600% worldwide [36]. One of the most common and persistent cyberattack vectors plaguing Smart Home IoT networks remains DoS attacks. As a result, this study focuses on DoS/DDoS attacks specific to SHIoT devices and network environments.

### 5.1 DoS/DDoS Attack Types

A Denial of Service (DoS) attack has the potential to obstruct the usage of legitimate users whilst rendering network resources unavailable and consuming bandwidth. Distributed denial of service (DDoS) attack is a type of denial of service (DoS) attack. In DDoS attacks, the attacker employs the use of several compromised systems to direct huge volumes of traffic in a synchronous and hierarchical manner which disrupts the normal traffic flow of the target system, network or application thereby overwhelming it and leading initially to a temporary denial of service, and subsequently a complete denial of service to genuine users of the network [37].

**Classification of DDoS Attacks in IoT.** Cyberattacks are mainly perpetrated using non-legacy IoT devices. However, the inherent vulnerability of these devices such as their low battery and computational capabilities, makes them susceptible to attacks [38]. Based on the reviewed literature, DDoS attacks within the IoT environment can be broadly classified into three (2) types: Layered attacks and Volumetric flood attacks. Figure 4 below shows the various types of DoS/DDoS attack types.



**Fig. 4.** DDoS Attack Classification in IoT.

Layered attacks are those attacks which target the application and Infrastructure layer of an IoT network and result in data packets being dropped and the magnitude is measured in Requests per second (Rps). Detecting and mitigating these attacks pose significant challenges as they generate traffic at a relatively low rate, disguising the malicious intent behind seemingly legitimate requests [39]. Despite appearing harmless, these requests disrupt backend IoT network processes that render resources inaccessible. Examples of such attacks include HTTP flooding and DNS amplification

attacks. The communication protocols at the application layer are a primary component of the IoT environment since they formulate the basis of all the interactions among IoT devices in the network [40]. As a result, to effectively counter application layer attacks, a flexible technique is critical. This strategy must entail the capability to modify traffic limitations based on specific sets of rules, which may be subject to periodic fluctuations.

Volumetric flood Attacks are primarily propagated by attackers sending a very high volume of traffic to an IoT network or device with the aim of depleting the network's resources such as bandwidth, memory, and CPU [14]. DDoS attacks can flood the victims' network through various methods, including SYN, TCP, UDP, ICMP flood attacks, Random IP Flood attacks, and Ping of death attacks.

*SYN flood attacks.* The SYN flood attacks, also known as half-open attacks, occur when an attacker deliberately refrains from completing the connection after making a request to the server. This strategy aims to exhaust the available server resources. The attack exploits the handshake process of a Transmission Control Protocol (TCP) connection, where TCP collaborates with IP to maintain data order between the sender and receiver [41]. During the handshake, the receiver receives a SYN packet from the sender to initiate the connection. It responds with an acknowledgement (ACK) and awaits another ACK from the sender. Instead of replying with a final ACK, the attacker persists in sending SYN packets until all available ports on the server are exploited [4].

*TCP flood attacks.* One of the most common DDoS cyberattacks is the TCP flood attack, which inundates the victim with a massive number of TCP connection requests without acknowledging the SYN-ACK of the victim server. This leaves the victim server with numerous half-open connections, consuming its resources and rendering it unavailable to authentic users [42].

*UDP flood attacks.* UDP flood attacks flood the victim network or device with many User Datagram Protocol (UDP) packets. The extensive volume of packets inundates the target server, aiming to overwhelm its processing and response capabilities. The mechanism of a UDP flood primarily capitalizes on the server's response process when it encounters a UDP packet directed at one of its ports. An example is the DNS amplification attack, where the attacker spoofs the source IP address of the victim and sends a small request to the DNS server. The DNS server replies with large responses, affecting the victim's performance [43].

*ICMP flood attacks.* The ICMP flood attack, also known as a Smurf attack, floods the victim server with many ICMP packets using spoofed source IP addresses. The victim server then responds to unsuspecting owners of the spoofed IP addresses with ICMP replies, affecting the performance and availability of both the victim server and the actual owners of the spoofed IP addresses [44].

*Ping of death.* A Ping of Death (PoD) attack is a type of DoS attack tactic where the attacker attempts to disrupt a victim device by directing a huge network packet surpassing the permissible size limit, thereby leading to the target device freezing or crashing [12].

## 5.2 Recommended Solutions and Mitigation Techniques

Several studies have been done around DoS/DDoS cyberattack detection/prevention which can accurately detect and prevent some intrusions/attacks. Table 2. below are a few of the common DDoS Cyberattack detection and mitigation techniques currently deployed in securing various types of IoT networks and devices.

**Table 2.** DDoS Cyber Attack Detection/Prevention Studies.

| Reference | DoS/DDoS Detection Mechanism                                        | Use case Target                                              | Papers covered |
|-----------|---------------------------------------------------------------------|--------------------------------------------------------------|----------------|
| [42]      | Open Flow statistics (Anomaly-based detection)                      | Simulated Software Defined Network (SDN) Environment         | 2013 - 2019    |
| [44]      | Machine learning model (Anomaly-based detection)                    | Simulated Software Defined Network (SDN) Environment         | 2015 - 2019    |
| [45]      | Fair Rate Throttling Mechanism/ Anomaly Detection Mechanisms        | Simulated Autonomous Systems (ASes)                          | 2005 - 2018    |
| [46]      | Hybrid Detection (Signature-based & Anomaly-based detection)        | Simulated IoT Network Environment                            | 2013 - 2019    |
| [47]      | Soft computing-based autonomous detection (Anomaly-based detection) | Hidden Markov model/ Simulated IoT Cloud Network Environment | 2007-2019      |

DoS/DDoS detection and prevention techniques are majorly categorised into; Anomaly-Based, Signature-Based & Hybrid-Based systems. Figure 5. below depicts the various types of DoS/DDoS cyberattack detection methods.

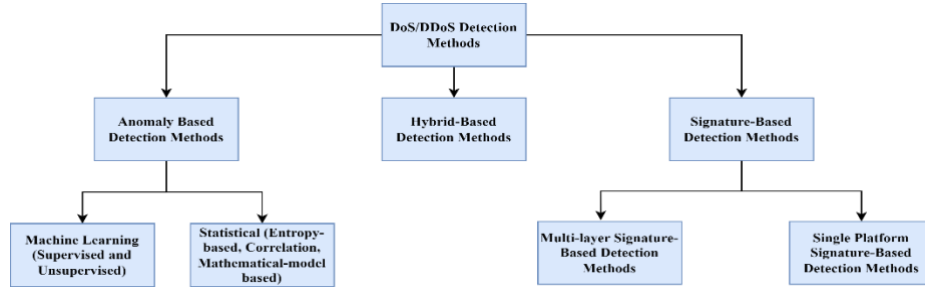


Fig. 5. Classification of DoS/DDoS Cyberattack Detection Methods

**Anomaly-based Methods.** Anomaly detection, also known as behavioural detection, involves identifying patterns or events that deviate from normal system behaviour [48]. To establish a baseline profile, network administrators generally observe network behaviour during non-attack periods. The primary objective is to detect subsequent patterns that diverge from this baseline. Initially, both malicious and non-malicious traffic data are collected and then forwarded to an anomaly detection module for analysis. When an anomaly is detected, an alert command is issued to the network operator, who then takes measures to mitigate or resolve the attack [49]. Various techniques, including data mining, statistical modelling, and hidden Markov models, have been employed by researchers for securing IoT networks. Researchers, Mugunthan et al. [47] proposed the use of soft computing-based autonomous detection for the Low-rate DDoS attacks. In the proposed technique, a Hidden Markov Model is deployed for monitoring the traffic in the network and the Random forest in differentiating suspected DDoS attacks from regular network traffic.

The Hidden Markov Model, which is a Stochastic model is used to forecast the likelihood of an attack happening. It consists of two states: the hidden state and the observational state. The attack severity levels obtained from the Hidden-Markov Model output are deployed in training the Random Forest to build a decision tree which in turn functions to detect abnormal network traffic. One advantage of this method is that it provides good accuracy and precision in the detection of low-rate DDoS in smaller networks. However, as with other Anomaly-based methods, the accuracy and precision significantly deteriorate as the network size is scaled up.

**Signature-based Methods.** Signature-based detection method relies on a record of known attack rules, monitoring network traffic patterns to identify a DDoS attack by comparing them with the database of patterns. When a similar traffic pattern is observed, it triggers a signal to the network administrator of the detection of an attack. This method demonstrates high detection accuracy when the rule database is regularly updated [37]. A Signature-based method for DDoS mitigation was proposed by Szykiewicz [50].

The approach uses packet generation algorithms (PGA) in the attack execution and carries out a protocol-level detection of DDoS traffic. Network traffic is monitored and verified against a set database of DDoS signatures. The implementation leverages

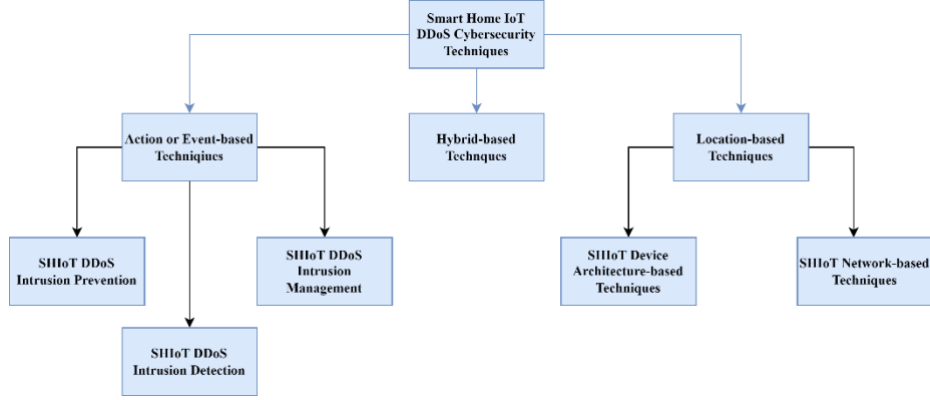
eBPF (extended Berkeley Packet Filter), a virtual machine with customized functionality. This solution offers a lightweight and portable approach. However, the overall user experience and accessibility of the proposed method are not easily replicable in other network environments and have no way of currently integrating other concepts.

**Hybrid-based Methods.** Hybrid-based detection methods combine anomaly-based and signature-based detection techniques. Hosseini and Azizi [51] proposed a hybrid framework for DDoS attack detection with the use of incremental learning.

A combination of machine learning algorithms including naïve Bayes, random forest, decision tree, multilayer perceptron (MLP), and k-nearest neighbours (K-NN) are also deployed in the proxy side to achieve detection. Each algorithm is tailored with specific features selected based on the behaviour of different attack types, enabling effective detection and enhanced capability to identify new attack variants. Advantages of the hybrid-based detection and mitigation approach are that each algorithm is tailored with specific features selected based on the behaviour of different attack types, thereby enabling effective detection and enhanced capability to identify new attack variants. However, one major drawback is that it requires a huge amount of computational resources, thereby slowing down the overall network performance and efficiency [52].

### 5.3 Classification of SHIoT DDoS Cybersecurity Techniques

The ideal scenario for SHIoT is when a DDoS attack never occurs to begin with. The unique topology of smart home-based IoT networks and the ubiquitous nature of SHIoT devices means that cybersecurity solutions have to be tailored specifically to suit their associated security challenges. Specifically, in relation to DDoS attacks targeting SHIoT, to the best of our knowledge, there appears to be very limited information on the classification or taxonomy of these attacks. As a result, from the reviewed literature, we have classified the various DDoS cybersecurity techniques into 3 major categories, namely, Action or Event-based techniques, Location-based techniques, and Hybrid-based techniques. Figure 9. below shows the various classifications of DDoS cybersecurity techniques for SHIoT.



**Fig. 6.** Classification of DDoS Cybersecurity Techniques for SHIoT.

**Action or Event-based SHIoT DDoS Cybersecurity Methods.** Action or event-based DDoS cybersecurity techniques are defined mainly based on the nature of the activity or event deployed and can be further categorised into SHIoT Intrusion Prevention, SHIoT Intrusion Detection, and SHIoT Intrusion Management.

*SHIoT Intrusion Prevention.* SHIoT Techniques are primarily aimed at or designed with the primary goal of preventing DDoS attacks from occurring. These techniques vary and several methods have been proposed by various researchers [53]-[55] including Model-based approach, Packet filtering, and Weight-fair throttling. Researcher James, [53] proposed an intrusion prevention system with the purpose of detecting and preventing the most critical forms of DDoS cyberattacks in different types of IoT smart home infrastructure. The proposed model-based approach functions by creating a set of controller policies which work to help thwart a DDoS attack. In instances where system or network administrators encounter false requests from SHIoT devices, services, or applications, the controller can enact policies to discard these false request packets or services. The approach is especially useful for preventing TCP flood attacks. However, one drawback of the approach is that it is not easily adaptable to cope with varied attack vectors not previously defined in the original controller policies.

*SHIoT Intrusion Detection.* SHIoT techniques are designed to detect DDoS attacks generally by comparing network traffic to a database of known signatures or by identifying anomalies in system behaviours or deviations from standard operating procedures [54]. These techniques include machine learning, and statistical or computational-based approaches. Intrusion detection methods based on machine learning independently learn patterns of irregular behaviour from attack datasets, without human intervention. Initially, machine learning algorithms are trained using data collated regarding cyberattack profiles, which is then utilized to construct a model. This model is subsequently employed to identify irregular traffic patterns or attacks within the actual SHIoT environment. Machine learning methods are generally

either supervised or unsupervised. Examples of machine learning methods include Bayesian Networks, Hidden Markov Models, Neural Networks (NN), Fuzzy Logic, and Decision Trees (DT) [56].

In statistical SHIoT intrusion detection methods, the system builds a statistical model for the normal behaviour of traffic. If the network traffic data deviates from the statistical model it is generally flagged as illegitimate. Several researchers have proposed various SHIoT intrusion detection methods [57]. Gajewski et al. proposed a smart home anomaly detection technique which deploys machine learning as a means of classifying and monitoring traffic data. It then correlates suspicious behaviour across the network resources at the service provider's data. The method utilizes a Naïve Bayesian (NB) model for parameter learning inference from input data consisting of monitoring records, each characterized as either normal or an anomaly. Upon detecting any anomaly within an individual packet flow, an alarm is triggered. Subsequently, the detected anomaly is annotated with information regarding devices that have participated in the suspected packet flow. The detected anomalies are then reported to the network administrator, and further processing is undertaken [58]. This approach is very useful in detecting ICMP and TCP flood attacks. However, one major drawback is that it is built on learning based on normal traffic activity profiles and modelled to only detect network traffic which deviates from the baseline profile as an anomaly. As a result, it struggles to detect new attacks that deviate from normal predefined attack profiles.

*SHIoT Intrusion Management.* As soon as a DDoS attack is identified, the standard response is to determine the nature of the attack, and its source and attempt to stop all traffic emanating from the source into the SHIoT network environment immediately. All compromised nodes are then removed from the network. There are several different approaches that are devised for tracing and identifying the real attack source. SHIoT Intrusion Management Techniques are primarily aimed at or designed with the primary goal of mitigating the effect of an already active DDoS attack [15]. Various attacks can disrupt the functionality of a smart home, including DDoS attacks, which typically overwhelm the network, resulting in interrupted communication. A more sophisticated form of DDoS attack targets a single IoT device, aiming to disable only a portion of the smart home services.

The capability of a smart home's network to effectively cope and to continue sending critical notifications to the users without too much interruption is outlined by Huraj et al. [59]. In their approach, a Fibaro device is used to continue sending notifications to the user's smartphone during a DDoS attack. The technique deploys two Z-Wave sensors (a motion sensor detecting movement in the monitored room, and a flood sensor triggered by potential flooding or abrupt temperature changes). One advantage of this technique is that it can easily mitigate the effects of SYN flood or UDP flood attacks. Despite an ongoing attack, hosts on the network can continue to perform with minimal interruptions and compromised nodes are isolated to prevent

disruptions. However, one major drawback is the inability of the system to be easily integrated with other smart home devices and networks.

**Location-based SHIoT DDoS Cybersecurity Methods.** Location-based DDoS cybersecurity techniques are defined mainly based on the architecture of the SHIoT or the layers of the SHIoT network where the DDoS attack occurs. Location-based DDoS cybersecurity techniques can be further categorised into SHIoT Device Architecture-based techniques and SHIoT network-layer-based techniques.

A vast majority of DDoS attack mitigation systems focus on the victim's end, as it bears the brunt of an attack. These systems include resource management and protocol security mechanisms. On the other hand, DDoS defence mechanisms deployed within the intermediate network prove highly effective, as they facilitate easy mitigation of attacks and enable attacks to be easily traced back to their origins. In some cases, DDoS defence mechanisms may be implemented within the source network if known and these help in boosting the capacity to intercept attacks before they reach the core network. One such mechanism is proposed by Al Bhayo et al. [60]. The technique is a Software Defined (SD-IoT) based framework designed to deliver security services to IoT networks. Within this framework, a programmable DDoS Attack Detection (C-DAD) application was developed. The C-DAD leverages counter values of various network parameters to detect DDoS attacks. The major advantage of the proposed technique is the ease of integration with other IoT network environments. However, the disadvantage is that CPU utilization fluctuates, and it requires a lot of network resources to function which leads to network attenuation and efficiency issues.

Kanber et al. proposed a three-level architecture designed to detect DDoS attacks at the application layer [61]. In the first level, the system selects optimal features from traffic samples. It then categorizes traffic as either regular traffic or an anomaly. Subsequently, the second level employs a hard voting classifier to determine the source of DDoS attack and the last level determines the type of DDoS attack type, distinguishing between UDP, TCP, or Mixed-based attacks. The technique is useful for early detection of attacks. However, the accuracy for detecting UDP attacks is very low.

**Hybrid SHIoT DDoS Cybersecurity Methods.** Hybrid SHIoT DDoS cybersecurity methods are a combination of Location-based and event-based DDoS detection methods. A two-stage detection scheme is usually deployed in this technique, although they prove to offer an added layer of security, hybrid solutions are notably slower when compared to other approaches. Also, in terms of the network overhead, hybrid methods require additional resources for executing multistage detection, when contrasted with other methods. Hybrid approaches offer easy adaptability, enabling them to adjust to new attack patterns from new data Mtawa et al. [62].

From the reviewed literature, several hybrid techniques have been proposed by various researchers [63]-[65]. A hybrid intrusion detection model for SHIoT (ID-SMART) is proposed by [65]. The proposed model uses two tiers for independently

detecting DDoS attacks. The first tier contains the random forests technique, while the second tier uses machine learning algorithms for intrusion detection. By combining the outputs of both tiers, it helps improve the overall DDoS detection accuracy. One major benefit of the system is that it can be easily integrated into other networks with varying traffic patterns due to the inherent design flexibility provided through the used decision combiner and the associated sensitivity parameter. However, major drawbacks of the system include the continuous need to train the anomaly detector, which poses a limitation on the overall system performance. Also, more sophisticated DDoS attacks may evade the tier one-based detector rules, which are generally known, and the system performance may degrade as the detection success mainly relies on machine learning algorithms for intrusion detection.

## 6 Conclusion

This paper presented a concise survey of prevalent smart home-based IoT and its associated security challenges. As the proliferation of smart home IoT devices has continued, it has become imperative to transcend traditional security approaches and comprehensively understand and address the diverse security issues inherent in smart homes. To this end, our study reviewed the current state of the art in DDoS attack detection strategy tailored for smart homes. The study also reviewed various cybersecurity approaches such as leveraging machine learning (ML) algorithms to identify DDoS Flood attacks. Based on the reviewed literature, we grouped these techniques into 3 major categories, namely: Event-based, Location-based & Hybrid-based SHIoT DDoS detection systems. The challenges associated with each of these techniques are also highlighted in this paper.

This classification differs from other existing cyberattack classifications since it is based on the location or nature of the cybersecurity events within a smart home network setup. Also, this study builds on previous literature, offering detailed analysis and insights that form a robust foundation for further research. By advancing the understanding of DDoS detection and mitigation, our work contributes to the development of effective cybersecurity models that safeguard smart home IoT networks from evolving cyber threats, ensuring the security of sensitive personal data and the reliable delivery of smart home services.

As part of our future research, we envisage extending this study to design a Scalable Trust-based DDoS attack detection model and evaluating this in a real-world setting. A system which identifies, collates, and makes security decisions based on trust values, and reputation that can establish the protocols for ensuring safety within an IoT network environment and subsequently detect anomalies. For instance, we plan to execute a trust-based model within a controlled network environment, confining the impact of DDoS attacks to this specific network setup with extended adaptability.

**Acknowledgements.** The authors would like to acknowledge the support of Nottingham Trent University (NTU) for a fully funded studentship.

**Disclosure of Interests.** The authors declare that there are no known financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

- [1] D. Buil-Gil *et al*, "The digital harms of smart home devices: A systematic literature review," *Comput. Hum. Behav.*, vol. 145, pp. 107770, (2023). Available: <https://www.sciencedirect.com/science/article/pii/S0747563223001218>. DOI: 10.1016/j.chb.2023.107770.
- [2] F. K. Aldrich, "Smart homes: Past, present and future," in *Inside the Smart Home* Anonymous (2003).
- [3] H. A. Tran *et al*, "SHIoT: A novel SDN-based framework for the heterogeneous Internet of Things," *Informatica*, vol. 42, (3), (2018).
- [4] S. Prajapati and A. Singh, "Cyber-Attacks on internet of things (IoT) devices, attack vectors, and remedies: a position paper," *IoT and Cloud Computing for Societal Good*, pp. 277-295, (2022).
- [5] A. Mihoub *et al*, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," *Comput. Electr. Eng.*, vol. 98, pp. 107716, (2022). Available: <https://www.sciencedirect.com/science/article/pii/S0045790622000337>. DOI: 10.1016/j.compeleceng.2022.107716.
- [6] R. Paudel, T. Muncy and W. Eberle, "Detecting DoS attack in smart home IoT devices using a graph-based approach," in *2019 IEEE International Conference on Big Data (Big Data)*, (2019). DOI: 10.1109/BigData47090.2019.9006156.
- [7] Y. Li *et al*, "IoT-apiscanner: Detecting api unauthorized access vulnerabilities of IoT platform," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, (2020).
- [8] J. H. Anajemba *et al*, "A counter-eavesdropping technique for optimized privacy of wireless industrial IoT communications," *IEEE Transactions on Industrial Informatics*, vol. 18, (9), pp. 6445-6454, (2022).
- [9] X. Liu *et al*, "Sniffmislead: Non-intrusive privacy protection against wireless packet sniffers in smart homes," in *Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses*. (2021).
- [10] S. Medileh *et al*, "A flexible encryption technique for the internet of things environment," *Ad Hoc Networks*, vol. 106, pp. 102240, (2020).
- [11] M. Humayun *et al*, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egyptian Informatics Journal*, vol. 22, (1), pp. 105-117, (2021).
- [12] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," in *2015 International Symposium on Consumer Electronics (ISCE)*, (2015). DOI: 10.1109/ISCE.2015.7177843.
- [13] P. Anand *et al*, "IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges," *IEEE Access*, vol. 8, pp. 168825-168853, (2020).
- [14] M. Schiefer, "Smart home definition and security threats," in *2015 Ninth International Conference on IT Security Incident Management & IT Forensics*, (2015). DOI: 10.1109/IMF.2015.17.

- [15] I. Cvitić *et al*, "Novel classification of IoT devices based on traffic flow features," *Journal of Organizational and End User Computing (JOEUC)*, vol. 33, (6), pp. 1-20, (2021).
- [16] L. Huraj, M. Šimon and T. Horák, "Resistance of IoT sensors against DDoS attack in smart home environment," *Sensors*, vol. 20, (18), pp. 5298, (2020).
- [17] I. Cvitić *et al*, "Smart home IoT traffic characteristics as a basis for DDoS traffic detection," in *3rd EAI International Conference on Management of Manufacturing Systems*, (2018).
- [18] H. A. Tran *et al*, "SHIoT: A novel SDN-based framework for the heterogeneous Internet of Things," *Informatica*, vol. 42, (3), (2018).
- [19] E. Anthi, "Detecting and Defending against Cyber Attacks in a Smart Home Internet of Things Ecosystem," *Detecting and Defending Against Cyber Attacks in a Smart Home Internet of Things Ecosystem*, (2022).
- [20] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," *Sustainable Engineering and Innovation*, vol. 3, (1), pp. 23-28, (2021).
- [21] T. A. Abdullah *et al*, "A review of cyber security challenges attacks and solutions for Internet of Things based smart home," *Int.J.Comput.Sci.Netw.Secur*, vol. 19, (9), pp. 139, (2019).
- [22] P. P. Gaikwad, J. P. Gabhane and S. S. Golait, "A survey based on smart homes system using internet-of-things," in *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*, (2015).
- [23] A. J. Obaid, "Assessment of smart home assistants as an IoT," *International Journal of Computations, Information and Manufacturing (IJCIM)*, vol. 1, (1), 2021.
- [24] S. Pirbhulal *et al*, "A novel secure IoT-based smart home automation system using a wireless sensor network," *Sensors*, vol. 17, (1), pp. 69, (2016).
- [25] R. O. Andrade, I. Ortiz-Garcés and M. Cazares, "Cybersecurity attacks on smart home during covid-19 pandemic," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, (2020).
- [26] H. Touqeer *et al*, "Smart home security: challenges, issues and solutions at different IoT layers," *The Journal of Supercomputing*, vol. 77, (12), pp. 14053-14089, (2021).
- [27] B. D. Davis, J. C. Mason and M. Anwar, "Vulnerability studies and security postures of IoT devices: A smart home case study," *IEEE Internet of Things Journal*, vol. 7, (10), pp. 10102-10110, (2020).
- [28] R. O. Andrade *et al*, "A comprehensive study of the IoT cybersecurity in smart cities," *IEEE Access*, vol. 8, pp. 228922-228941, (2020).
- [29] C. Withanage *et al*, "A comparison of the popular home automation technologies," in *2014 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA)*, 2014s.
- [30] Z. Shouran, A. Ashari and T. Priyambodo, "Internet of things (IoT) of smart home: privacy and security," *International Journal of Computer Applications*, vol. 182, (39), pp. 3-8, (2019).
- [31] Haque, M. R., Tan, S. C., Yusoff, Z., Nisar, K., Lee, C. K., Kaspin, R., & Memon, S. A novel DDoS attack-aware smart backup controller placement in SDN design. *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN, 2516-0281. (2020)s.
- [32] J. LaMarche *et al*, *Home Energy Management: Products & Trends*. (2022).

- [33] PurpleSec Homepage *10 Cyber Security Trends You Can't Ignore In 2021*. Available: <https://purplesec.us/cyber-security-trends-2021/> last accessed 2023/11/12.
- [34] A. Bhardwaj *et al*, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Computer Science Review*, vol. 39, pp. 100332, (2021).
- [35] N. Agrawal and S. Tapaswi, "Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, (4), pp. 3769-3795, (2019). DOI: 10.1109/COMST.2019.2934468.
- [36] F. Hussain *et al*, "IoT DoS and DDoS attack detection using ResNet," in *2020 IEEE 23rd International Multitopic Conference (INMIC)*, (2020).
- [37] G. Nebbione and M. C. Calzarossa, "Security of IoT application layer protocols: Challenges and findings," *Future Internet*, vol. 12, (3), pp. 55, (2020).
- [38] N. M. Yungaicela-Naula, C. Vargas-Rosales and J. A. Perez-Diaz, "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," *IEEE Access*, vol. 9, pp. 108495-108512, (2021).
- [39] N. Ahuja and G. Singal, "DDoS attack detection & prevention in SDN using OpenFlow statistics," in *2019 IEEE 9th International Conference on Advanced Computing (IACC)*, (2019).
- [40] A. Y. Nur, "Combating DDoS attacks with fair rate throttling," in - *2021 IEEE International Systems Conference (SysCon)*, 2021. DOI: 10.1109/SysCon48628.2021.9447054.
- [41] O. Rahman, M. A. G. Quraishi and C. Lung, "DDoS attacks detection and mitigation in SDN using machine learning," in *2019 IEEE World Congress on Services (SERVICES)*, (2019).
- [42] A. Y. Nur, "Combating DDoS attacks with fair rate throttling," in *2021 IEEE International Systems Conference (SysCon)*, (2021).
- [43] M. M. Shurman, R. M. Khrais and A. A. Yateem, "DoS and DDoS attack detection using deep learning and IDS." *Int.Arab J.Inf.Technol.*, vol. 17, (4A), pp. 655-661, (2020).
- [44] S. R. Mugunthan, "Soft computing based autonomous low rate DDOS attack detection and security for cloud computing," *J.Soft Comput.Paradig.(JSCP)*, vol. 1, (02), pp. 80-90, (2019).
- [45] A. Banitalebi Dehkordi, M. Soltanaghaei and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *The Journal of Supercomputing*, vol. 77, pp. 2383-2415, (2021).
- [46] C. Douligieris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: A classification," in *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. no. 03EX795)*, (2003).
- [47] P. Szynekiewicz, "Signature-based detection of botnet DDoS attacks," in *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools* Anonymous (2022).
- [48] S. Hosseini and M. Azizi, "The hybrid technique for DDoS detection with supervised learning algorithms," *Computer Networks*, vol. 158, pp. 35-45, (2019).
- [49] S. Nandi, S. Phadikar and K. Majumder, "Detection of DDoS attack and classification using a hybrid approach," in *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, (2020).

- [50] F. James, "IoT cybersecurity based smart home intrusion prevention system," in *2019 3rd Cyber Security in Networking Conference (CSNet)*, (2019).
- [51] K. Al-Begain *et al*, "A DDoS Detection and Prevention System for IoT Devices and Its Application to Smart Home Environment," *Applied Sciences*, vol. 12, (22), pp. 11853, (2022).
- [52] M. Sharma and B. Arora, "Detection and prevention of DoS and DDoS in IoT," in *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security: IC4S 2020*, (2021).
- [53] M. Yamauchi *et al*, "Anomaly detection in smart home operation from user behaviors and home conditions," *IEEE Transactions on Consumer Electronics*, vol. 66, (2), pp. 183-192, (2020).
- [54] A. Sgueglia *et al*, "A systematic literature review of IoT time series anomaly detection solutions," *Future Generation Comput. Syst.*, vol. 134, pp. 170-186, 2022.
- [55] M. Gajewski *et al*, "Anomaly traffic detection and correlation in smart home automation IoT systems," *Transactions on Emerging Telecommunications Technologies*, vol. 33, (6), pp. e4053, (2022).
- [56] L. Huraj, M. Simon and J. Lietava, "Smart home defense against DDoS attacks," in *Proceedings of the Computational Methods in Systems and Software* Anonymous (2022).
- [57] 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).
- [58] B. M. Kanber *et al*, "DDoS Attacks Detection in the Application Layer Using Three Level Machine Learning Classification Architecture." *International Journal of Computer Network & Information Security*, vol. 14, (3), (2022).
- [59] Y. Al Mtawa *et al*, "Smart home networks: Security perspective and ml-based DDoS detection," in *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, (2020).
- [60] L. Shi, L. Wu and Z. Guan, "Three-layer hybrid intrusion detection model for smart home malicious attacks," *Comput. Electr. Eng.*, vol. 96, pp. 107536, (2021).
- [61] V. Subbarayalu, B. Surendiran and P. Arun Raj Kumar, "Hybrid network intrusion detection system for smart environments based on internet of things," *The Computer Journal*, vol. 62, (12), pp. 1822-1839, (2019).
- [62] F. Alghayadh and D. Debnath, "A hybrid intrusion detection system for smart home security," in *2020 IEEE International Conference on Electro Information Technology (EIT)*, (2020).