DENIAL OF SERVICE ATTACKS, ITS SIGNIFICANT AND CURRENT TRENDS TO INTERNET OF THINGS

By

OYEBOLA OYELOWO

CYBERSECURITY PRINCIPLES

TABLE OF CONTENTS

INTRODUCTION

1.1 BACKGROUND AND SIGNIFICANCE

Over the last decades, the Internet of Things (IoT) has taken a sporadic technological revolutionary shift in objects of everyday life, offering a wide range of applications across various industries including the advent of smart cities, agriculture, health systems, smart transport systems, smart grid system, education, environmental and weather monitoring systems, supply chain system which are an important factor in a digital economic development world. Wi-Fi is a widely utilized technology for the wireless connection of IoT devices because of its widespread deployment and inexpensive cost (Sheth et al., 2019). Otoum et al. (2022) report that the amount of connected devices is estimated to rise from 27 billion in 2017 to 125 billion in 2030, giving an average increase of 12%.IoT devices include essential components including):

1. **Sensors:** sensors are used to respond to environmental conditions. It plays an important role in IOT because it senses and interprets data in real time and converts it to electric or digital signals to be transmitted to a central hub or cloud-based system for processing (Sheth et al., 2019). For instance, motion sensors respond to movement within their environment
2. **Microprocessors:** The microprocessor can be likened to the brainbox of smart devices. They control the operation of IOT devices such as temperature switching regulations collecting and processing data perceived by the sensors, removing excessive junk and compressing the data where necessary before sending it to the memory (Sheth et al., 2019).
3. **Memory:** The memory is the database of the IOT devices where storage of data collected and operations are stored. Sensors temporarily store data recorded to the memory before storing it in the central hub or the cloud. The memory sizes vary based on specific applications and devices (Sheth et al., 2019).
4. **Communication Channels:** These are channels through which IOT devices interact with other devices and the internet. They can include Cellular, Wi-Fi, Bluetooth,
5. **Power Supply:** This is a critical component that influences IoT devices. It determines the battery life, power efficiency and environmental impact.

6. **User Interfaces:** These are the output devices that allow user interactions. They may be touchscreen devices or audio devices like laptops, smartphones and tablets.

IoT devices consist of three layers which are the Network Layer, Application Layer and Perception layer (Varadharajan et al., 2018). Table 1 presents the driving protocols used at different layers.

LAYER NAME	**Brief explanation**	**PROTOCOL USED**
Application Layer	It represents the IoT data processed. They are vendor-specific and are designed to handle individual IoT. They can be run on end devices like smartphones (Varadharajan et al., 2018).	MQTT-SN, XMPP, HTTP REST, HTTP, CoAP, DDS, AMQP, MQTT.
Network Layer	Transmits data throughout the IoT devices. It can be transmitted wirelessly or wired. Examples, are ZigBee, Wi-Fi, and Bluetooth (Varadharajan et al., 2018).	MDNS, DNS-SD, RPL, 6LoWPAN, IPv4/IPv6.
Perception Layer	includes the sensors and actuators that are used to monitor the physical environment and control the activities of the physical devices, Examples are motion sensors and air cooler control (Varadharajan et al., 2018).	IEEE 802.15.4, Z-Wave, EPCglobal, LTE-A.

Table 1: IOT Architecture (Varadharajan et al., 2018).

Source: Varadharajan et al., 2018.

The IoT concept emerged in the late 20th century when Kevin Ashton, a British technologist, introduced the term "IoT" in 1999 (Bansal et al., 2021). The idea envisioned a network where physical objects could be equipped with sensors, connected to the internet, and share data seamlessly (Bansal et al., 2021). However, the practical implementation of IoT gained momentum in the 2000s with advancements in sensor technology, wireless communication, and cloud computing. The convergence of these technologies allowed for the widespread deployment of connected devices, enabling real-time data collection, analysis, and remote control. Over the years, IoT has become a transformative force across industries, impacting fields such as healthcare, transportation, agriculture, and smart cities (Hassan et al., 2022). The continued evolution of IoT involves addressing challenges related to security, interoperability, and scalability as the interconnected ecosystem continues to grow (Marykyan et al., 2018).

In the cyber era, the IoT environment is experiencing a lot of privacy and security issues). There are no security and privacy standards by government bodies to govern IoT industries to design IoT devices (Safavi et al., 2019; Marykyan et al., 2018). Furthermore, the complexities of IoT devices have increased the challenges of IoT devices. Therefore, privacy and security are major challenges to the IoT and have various vulnerabilities including link spoofing, man-in-the-middle, dictionary, brute force and relay which makes IoT-based IoT architecture extremely unsafe. It is very important to first identify and then analyze potential security concerns in order to develop a complete picture of the security status of an IoT-based IoT system (Heartfield et al., 2018).

1.2 Applications of IoT

IoT has become prevalent and it is now becoming an important part of our daily lives providing us with a better quality of life, convenience, efficiency and security (Jalal et al., 2019).

IoT are connected to the internet and are communicated and controlled remotely with minimum human intervention and supervision to allow convenience, a budget-friendly better quality of life and enhanced security (Jalal et al., 2019). For example, in smart cities, smart agriculture, and smart locks card reader, with a smart light bulb, users do not have to stress themselves switching from the socket when they can control it simply by their presence or voice command and by our phones. These devices communicate with one another and synchronize their activities (Gupta et al., 2022).

1.3 Security Challenges Associated with the IoT

IoT devices are designed with functionality in mind and building rather than security and manufacturers do not educate the users about the vulnerabilities of their products. Thus, it is prone to vulnerabilities like lack of updates, remote control, physical attacks, communication errors and other unforeseen bad connections amongst the connected devices (Mishra et al., 2021).

Furthermore, the main objective of an attacker of IoT is to infiltrate the system to steal valuable information from the system and steal data patterns or daily information to study the daily usage of the household and use it to steal confidential information or plan a burg. The attacker can also manipulate any vulnerable devices to gain control of the IoT devices like avoiding trigger alerts and in extreme cases, running a Mirai to execute a DDoS attack against smart devices and websites (Sinanović et al., 2017).

All possible IoT challenges can be classified according to the STRIDE scheme and detailed in table 2 (Araya et al., 2023):

Threat	**Property**	**Definition**	**Example**
Spoofing	Authentication	Pose as something or somebody else, such as legitimate users, processes, or system elements	An attacker spoofs the MAC address of a smart device to gain access to a network.
Tampering	Integrity	Modification or edition of legitimate data or code.	An attacker who manipulates the firmware of an IoT device to gain unauthorized access to the device or the network.

Repudiation	Non-Repudiation	Denying to have performed a particular action than other parties can neither ratify nor refuse	A user denying having issued certain commands to the automation system, despite evidence suggesting otherwise
Information Disclosure	Confidentiality	Data breach or unauthorized access to confidential information.	An attacker intercepts and reads sensitive information such as user credentials, network traffic or sensor data from an IoT system, leading to potential privacy violations and unauthorized access.
Denial of Service	Availability	Interruption of service to legitimate users	An attacker overwhelms a smart device with traffic so it cannot function properly
Elevation of Privilege	Authorization	We are obtaining higher privileged access to system elements by a restricted user.	An attacker gains elevated access to an IoT device by exploiting a vulnerability in its firmware, allowing them to perform actions beyond their intended level of access.

Table 2: The STRIDE Scheme (Araya et al., 2023)

Source: Araya and Rifa-Pous (2023, p3)

1.4 Security Attacks Associated With IoT Devices

IoT devices are susceptible to various security attacks at each layer of IoT devices, these give an overview of how cyber attackers can intrude and take advantage of the IoT security challenges and gain complete control of the network which are:

1) **Application Layer:** It acts as a bridge between the network and the IoT devices all application and service IoT devices are embedded in the application layer. These applications and services include defining the scope of the devices including least privilege, and scale repeatability. IoT devices like other IoT devices are designed primarily for the effective operation of their products rather than protecting the security of the device. Therefore, the application layer can be vulnerable to the following attacks:

    1) **Brute force Attacks:** Most IoT devices come with default passwords which are mostly known by all including the attackers and users mostly use weak passwords including , date of birth, phone numbers and name-related passwords to remember the password easily and with brute force, cyber attackers can attempt all possible password combinations and encryption keys (Chen, K et al., 2018). It is an attack against the user login details thereby exploiting the confidentiality, integrity, authenticity and authorization of the IoT device.
    2) **Phishing: A**ttackers can use social engineering to manipulate users to divulge sensitive and confidential information such as login details and financial information which could be in the form of an email phishing or vishing, and they could ask users to install a fake application on their device (Alharbi et al., 2022). Phishing attacks affect the confidentiality, availability, and authenticity of IoT devices
    3) **Malware:** Sending malicious software such as a false link or fake application can be used to infiltrate the IoT networks and as bait to receive sensitive information from users and It could be in the form of ransomware, or viruses. Injecting malware into the devices can also trigger other types of attacks (Wazid et al., 2019).
    4) **Code Injection:** Code injection is an act of injecting malicious codes into IoT applications that are vulnerable to exploit the system and manages

    authorization by granting access to unauthorized entities (Ali et al., 2018), it aims to exploit confidentiality and escalate the privacy of IoT application, hence the network.

    5) **Man in the Middle Attack (MiTM):** Attacker has a direct influence on the users. It could be actively or passively monitors and manipulates communication between IoT devices using several methods like IP address spoofing, attaches itself between them, and capture sensitive information or intercepts and insert new information (Fereidouni et al., 2023).

2) **Network Layer:** Network layers transmit information from the perception layer using a wired or wireless medium like Bluetooth and Wi-Fi. The vulnerabilities involved in this layer include the following:

    1) **IP address Spoofing:** IP address spoofing is an attack on impersonating and manipulating a source IP Address of a device in a network to manipulate and deceive the network (Mohammadnia et al., 2020).

    2) **Mac Address Spoofing:** MAC address spoofing is an attack network to manipulate and deceive the network by impersonating and manipulating a source MAC Address of a device (Mohammadnia et al., 2020).

    3) **Packet Sniffing:** This is an attack where an attacker manipulates and monitors data communication, Network information can be intercepted and it can lead to loss of information even though it can be used for troubleshooting purposes, it can also be a security attack used for malicious purposes (Chen, K et al., 2018).

    4) **Replay Attack:** the attacker intrudes, eavesdrop, intercept and record the data transmission to replay repeatedly at other times to obtain network-related information between the devices (Chen, K et al., 2018), it can cause the exhaustion of the network.

    5) **Denial of Service Attack/ Distributed Denial of Service (DDoS)**: This attack disrupts the availability and accessibility of legitimate users, it is they are both synonymous, however, with distributed denial of service, the attack comes from a collection of botnets targeted towards the destination devices (Yang et al., 2017).

3) **Perception Layer:** This is the physical aspect of the network where the physical connection takes place using Ethernet or cables. It consists of the physical devices that are connected to the internet connection including RFID chips and sensors (Hu et al., 2018).

    1) **Physical Tampering**: This is unauthorized access to physical devices or hardware components such as CCTV cameras, computers, routers, and servers. Which can lead to the replacement of the device or alter the component of the server to exploit vulnerabilities in the system (Hu et al., 2018).
    2) **Side Channel Attack:** attackers exploit a network or device's physical qualities like power consumption and timing rather than its vulnerabilities and aim to extract sensitive data using the hash function (Ghazar et al., 2020).
    3) **Worm Hole Attack:** these are two or more malicious end devices connected to create a wormhole tunnel, each end devices receive data from their neighboring nodes and forward them to the wormhole tunnel in another location within the network while altering the data sent, they can be closed, half-opened and opened wormholes (Ibrahim et al., 2021).
    4) **Eavesdropping:** this attack can have a significant impact on confidentiality, authorization and data privacy of the network that highly relies on a wireless medium of communication, it intercepts and monitors the private and sensitive communication between nodes without authorized access (Khoo, 2011). The broadcasting nature of the wireless medium makes wireless communication in IoT systems, including uplink and downlink communications, extremely susceptible to eavesdropping assaults (Khoo, 2011).
    5) **Spoofing Attack:** the attacker disguises himself as authentic to gain permission and access to the communication channel. It may lead to packet loss in the transmission process (Chen et al., 2018).

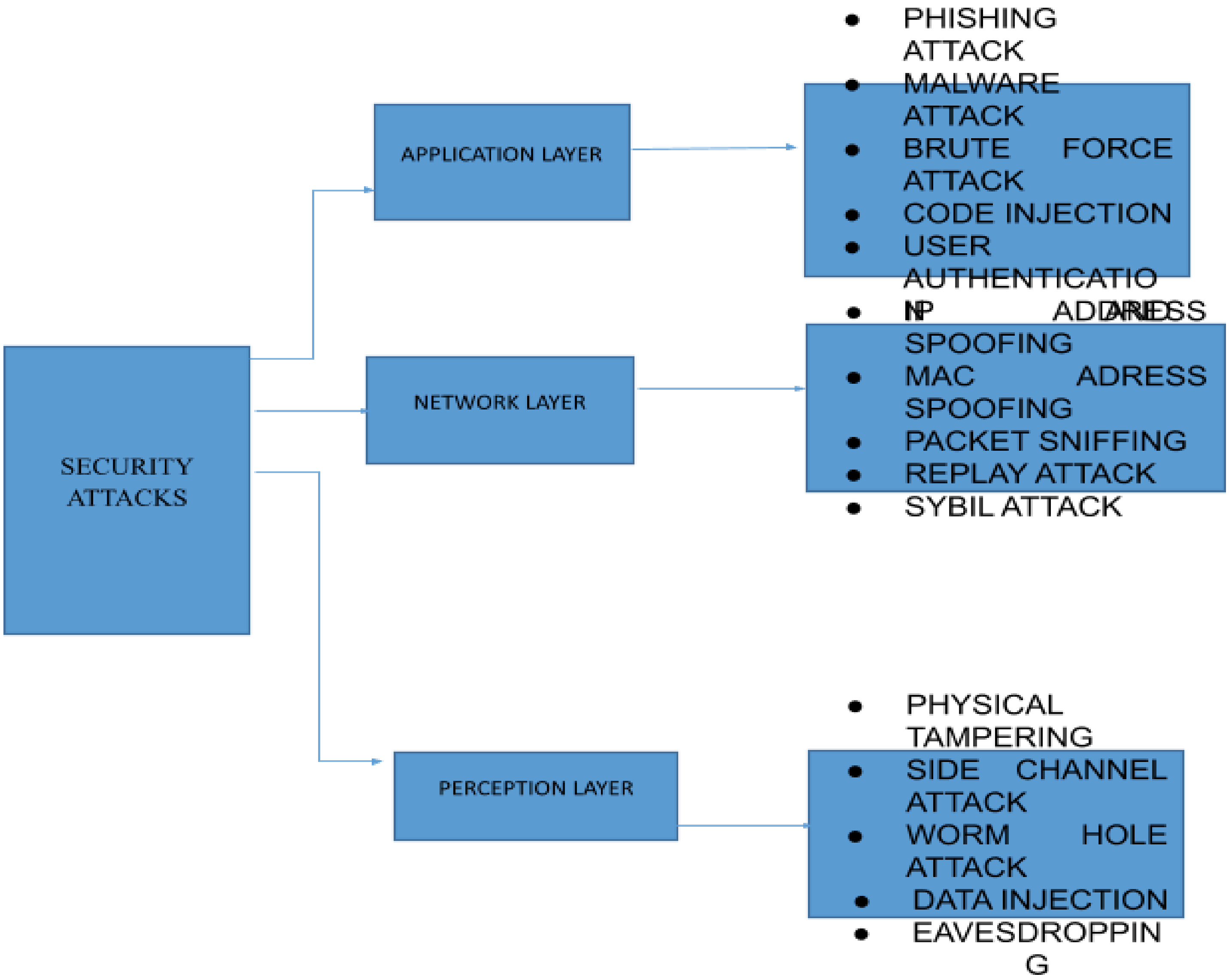

Figure 1: Types of security attacks.

Source: Oyebola Oyelowo

Adapted From: Inaya et al., (2016, p 458)

Selected Security Challenge, (Distributed Denial of Service)

Distributed Denial of service (DDoS) attack is a prevalent security attacks in recent years where an attack makes use of a botnet to flood the server or the smart device with simultaneous requests thereby overwhelming the device. DDoS attack is one of the most dangerous challenge to the internet and the amount of these type of attacks increases annually (Emina et al., 2019).

2.1 LITERATURE REVIEW

In this session, a deep understanding of the denial of service attack as a common attack that is prevalent in IoT devices will be established, it will begin with an overview of the denial of service attacks, the motivation behind the DDoS attacks and the techniques used in DDoS attack and their significance to IoT devices, including communication protocols and associated vulnerabilities, and types of denial of service attacks.

Furthermore, historical cases of DDoS attacks on IoT devices will be presented, including attack vector techniques and their impact on IoTs. Continuing into the mitigation techniques for DDoS attacks will be clearly stated as challenges that are being faced and recommend a better approach to secure IoT devices, concluding with an analysis of case studies and potential solutions for enhanced security.

2.2 Overview of DDoSAttack And Its Significance To The IoT

The IoT influences everyone’s daily life and their adaptation and comfortability has significantly increased, it consists of components which aid communication with one another using interconnected devices such as switches and routers (Tushir et al., 2021). It is called smart because users can control and interact with it remotely via the internet and end devices like laptops or tablets (Karimi, 2019). However, IoT have a lot of vulnerability, especially in their communication protocol which attackers have also found as a useful weapon for exploitation to generate a large number of botnet to execute the most dangerous attack on the internet - The Distributed Denial of Service (DDoS) (Gupta et al., 2022).

The DDoS attack is an attack that disrupts the flow of communication of users' devices and services on the internet and within the network by compromising the bandwidth of the targeted network through flooding of traffic from different sources. It is most achieved using an IP gateway including interconnected devices like routers and switches (Sheth et al., 2019). IoT devices rely on Wi-Fi connectivity due to their wide deployment and low cost (Sheth et al., 2019).

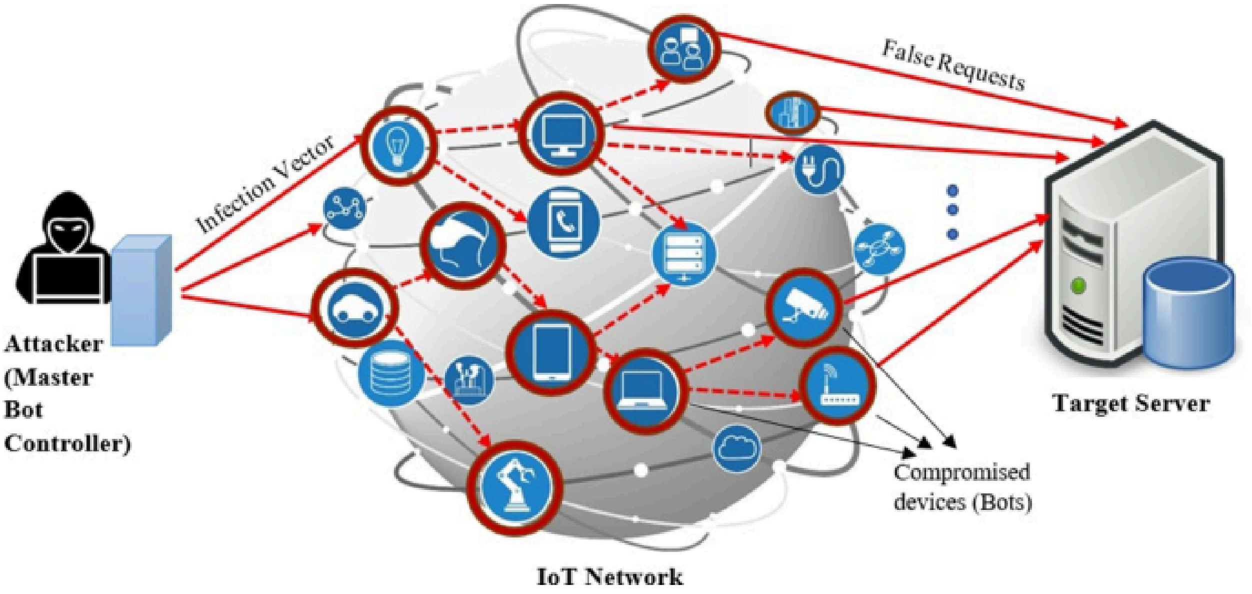

Figure 2: DDoS Attack Using IoT Weapon (Vishwakarma et al, 2019)

Source: Vishwakarma et al, 2019.

Figure 2 explains how DDoS attacks happen, the attacker creates a Master Bot and forms a network of Botnet, then targets vulnerable IoT device and compromise it, and these devices are always internet-connected afterwhich the attacker then instructed the botnet to send large numbers of malicious codes to the targeted device or network through the botnets to excessively flood the network (Gupta et al., 2022; Vishwakarma et al., 2019).

According to Google Cloud, (2023), Google's DDoS response team has observed an exponential increase in the expansion of DDoS attacks, In June 2022, the largest layer 7 HTTP DDoS attack was reported which peaked at forty-six (46) million requests per second making it 76% larger than the previous attack recorded with twenty-six (26) million requests per second, Also, 690 mega network packet per second attack were reported to be generated by IoT botnet in 2022 and another attack in 2015 on a customer's virtual machine which an IoT botnet was expanded up to

445 Mega network packet per second in 40 seconds (Omer Yoachimik, 2022). Figure 3 shows the graphical representation of DDoS in the last decade.

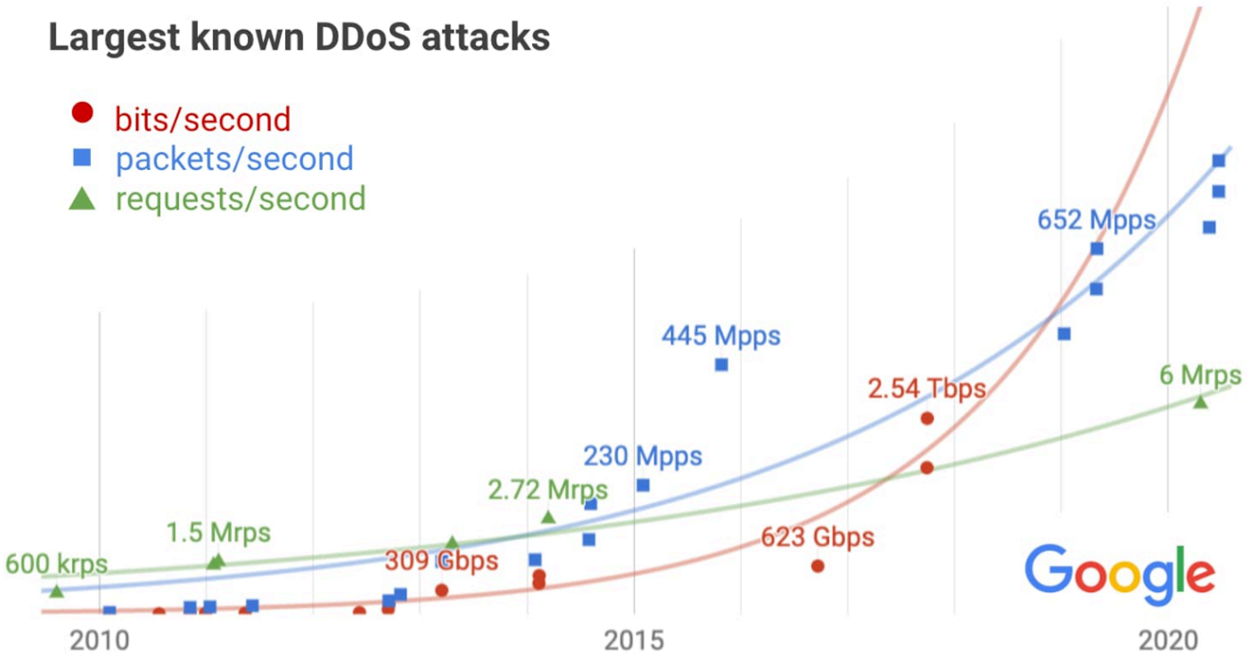

Figure 3, Analysis of DDoS Attacks in the Last Decades

Sourced From: (Google Cloud, 2020)

From the analysis in Fig 1, the rate of DDoS attacks keeps doubling up with the number of years with alarming metrics from (2010-2020).

2.3 Types of DDoS Attacks

The types of DDoS attacks mostly occur at the Application and Network layer though it can also occur at the perception layer.

1. **Network Layers:** These attacks target the network infrastructure, communication protocols and interconnected devices. These attacks are:
   1) **UDP Flood Attack**: Most IoT devices depend on UDP connection because communication is in real-time with low latency and synchronization even though it is connectionless and non-reliable, he attacker generates various UDP packets from spoofed IP addresses and floods them to the targeted devices and network through the botnets generated (Liu et al., 2019).

2) **ICMP Flood Attack**: It is also called Ping to Death, the attacker sends ICMP echo requests to the targeted device from a different source IP address knowing that there will be many reply packets as there will be request packets which results in flood attack (Gupta et al., 2022).

3) **SYN Flood Attack**: SYN/ACK is a three-way handshake that occurs in the TCP/IP communication protocol, SYN/ACK flooding occurs when the attacker floods the target device with many SYN/ACK packets from different spoofed IP addresses, the targeted device opens multiple ports until it is exhausted and the number of ports available becomes zero which leads to a form of distributed denial of service attack (Gupta et al., 2022).

2. **Application Layer:**

1) **HTTP/HTTPS Flood Attacks**: The attacker sends different HTTP GETs and POSTS requests from various devices and uses legitimate HTTP GET or POST requests to begin a DDoS attack thereby processing a lot of data on the server side and puts load on the server resources, thereby denying access to legitimate users (Gupta et al., 2022; Ibrahim et al., 2022).

2) **Mobile App-Based Attacks**: Mobile applications interact with the internet, cloud, access data and services using the API. First, the attacker finds the API that supports the mobile application, then sets up a botnet and commands it to generate massive API calls to flood the target network. Thereby exhausting the bandwidth and memory and causing unavailability to the target device and network (Yang et al., 2017).

3) **Resource Depletion Attack:** These resources can be in the form of data packets, bandwidth, processors, database resources, API, firewalls, CPU, and memory, this attack is achieved by sending much traffic to the targeted device of the network and overwhelming the targeted device, expending the CPU and routing high volume of traffic which can stress the memory capacity (Yang et al., 2017).

4) **DNS Amplification:** the attacker sends malicious code to the botnet to generate and control the domain’s DNS server with requests to distrupt DNS resolution which makes it impossible for the server or API to respond to legitimate traffic (Ibrahim et al., 2022).

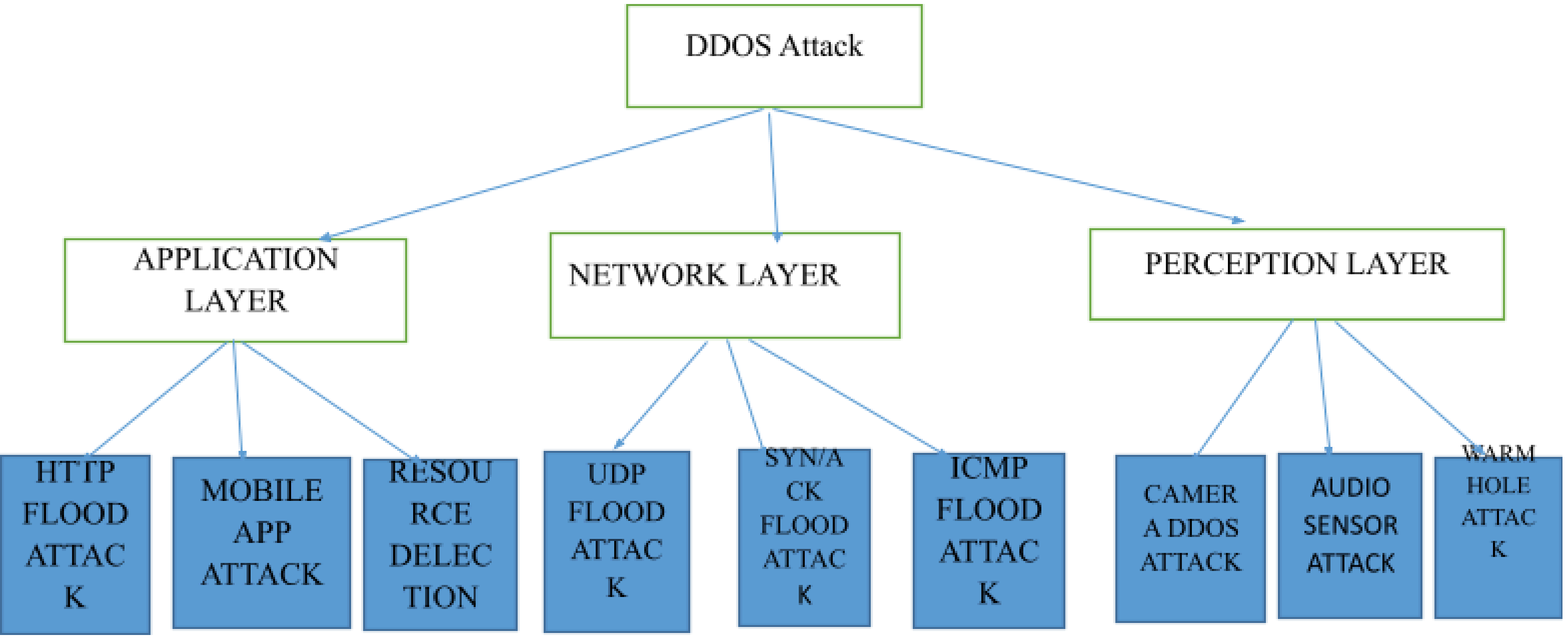

Table 3: DDOS Attacks

Source: Oyebola Oyelowo.

2.4 Related Works on Current Trends and Solutions

In the last decade, there has been an emergence of solutions to mitigate DDOS attacks. However, in the last five years, technologies like blockchain technology, SDN, Fog Computing and machine learning offered solutions (Surianarayanan et al., 2023). This paper explores different researchers' views on mitigating DDoS attacks according to the algorithm and techniques used:

The propagation of DDoS Attacks in IoT and the use of Software Defined Networking to detect and mitigate DDoS Attacks, proposed a framework called ProDefense that is used in smart cities, this framework is designed to meet application-specific requirements for DDoS attack detection and mitigation, the document also discusses open research challenges and future directions for improving detection and mitigation capabilities (Bawany et al., 2017).

According to Lawal et al. (2020) a DDoS Mitigation framework includes a database for storing previous attacks, which enables fast and accurate attack detection; moreover, it detects DDoS attacks through a Fog Computing based K-NN classification algorithm: therefore, this kind of mitigation framework is an anomaly-based intrusion detection method and database

A novel security scheme consists of a decentralized cloud-based SDN architecture and a machine learning algorithm that detects and mitigates DDoS attacks in IoT networks called LEDEM and was tested with testbed topologies and in real hardware network and compared with other models such as Dee Belief Networks, Native Bayes and Extreme Learning Machine and it achieved a more precise accuracy than the others achieving an outcome of 96.28% accuracy detected DDoS attacks (Ravi, 2020).

In utilizing blockchain technology to mitigate DDoS attacks, the categorization and classification of the existing mitigation of DDoS attack strategies using blockchain technology based on Nera Victim Location, Hybrid Solutions, Network Level Mitigation and Near Attack Domain Location was proferred, the research challenges associated with blockchain including the dearth of peer-to-peer network datasets, zero-day vulnerabilities and detecting spoofed IP DDoS attacks, the adoption of the blockchain internet, programmable data planes for blockchain-based DDoS solutions, blockchain-based threat information sharing, and the

Ethereum 2.0 network's application for DDoS mitigation are among the future research objectives he delineates (Rajasekhar et al., 2022).

Multilevel Distributed Denial of Service (ML-DDoS) is another reliable framework for mitigating DDoS attacks in the IoT using smart contracts and blockchain technology and uses blockchain technology to reduce the number of rogue IoT devices, in comparison to previous methods, the framework demonstrated improves latency, throughputs, and CPU utilization when examined using benchmark programs (Hayat et al., 2022).

Yakubu et al. (2023) presented a blockchain mitigation protocol against DDoS attacks in IoT devices which utilizes the Ethereum blockchain and smart contract to secure device-to-device (D2D) communication using a lightweight authentication medium and single server queueing system model to preclude DDoS attacks, the result confirms the protocol effectively protects against internal collision attacks and is a scalable and efficient technique for reducing DDoS attacks in IoT networks (Yakubu et al., 2023).

Kaur et al. (2023) leveraged the analysis from different authors to recommend the taxonomies for the attack mechanisms and the defence techniques and summaries various DDoS attacks in recent technologies including the Internet of Things (IoT), It further presented several defense mechanisms including SDN to secure the data plane, and data-control plane communication channel, control plane, (Kaur et al., 2023).

Authors	**Mitigation Type**	**Research Works**	**Keywords**
Bawany et al., 2017	Software-Defined Networks	Proposed a framework called ProDefense for uses SDN to detect and mitigate DDoS attacks against DDoS attacks in smart cities (Bawany et al., 2017).	OpenFlow, DDoS mitigation , Software-defined networking, DDoS attacks (Bawany et al., 2017).
Lawal et al, 2020	Fog Computing	Presented an anomaly-based intrusion detection uses a K-NN classification algorithm for	Fog computing , Internet of Things (IoT),

		detecting DDoS Attacks (Lawal et al., 2020).	Anomaly mitigation DDoS (Lawal et al., 2020).
Ravi, 2020	machine learning algorithm and a decentralized cloud based SDN architecture	Proposed LEDEM that detects and mitigates DDoS attacks in IoT networks called LEDEM (Ravi, 2020).	DDoS attacks, Software-defined networking (Ravi, 2020).
Chaganti et al., 2022	Blockchain Technology	Classified the existing mitigation of DDoS attack strategies using blockchain technology based on Network Level Mitigation, Near Attack Domain Location, Nera Victim Location and Hybrid Solutions (Chaganti et al., 2022).	Blockchain, Denial of service attack, DDoS attacks, Internet Service Provider, IoT, Software Defined Networks, Smart contract, (Chaganti et al., 2022).
Hayat et al., 2022	Smart Contracts and Blockchain Technology	Multilevel distributed Denial of Service (ML-DDoS) method to reduce the number of rogue IoT devices (Hayat et al., 2022).	Cybersecurity, Blockchain, DDoS, IoT, Artificial Intelligence, Attacks, (Hayat et al., 2022).
Yakubu et al., 2023	Blockchain technology	protocol utilizes the Ethereum blockchain and smart contract to, protects	Ethereum, DDoS attack, Authentication,

		against internal collision attack (Yakubu et al., 2023).	Blockchain, Device-to-device Smart homes, smart contract (Yakubu et al., 2023).

Table 3: Current Trends to Mitigating DDoS Attacks

Source: Oyebola Oyelowo

3.0 CRITICAL THINKING

These methods to mitigate DDoS attacks are brilliant and evolving; however, most of these current trends take a defensive and preventive approach to mitigate DDoS attacks, while this is good, this paper suggests a proactive approach towards both the technical side and the user side is equally significant because users are equally a major factor in mitigating DDoS attacks.

During the development phase, security should be considered alongside functionality and comfortability. IoT devices should have firewalls configured with them at the development stage. Moreover, installing DDoS protection services that pick up and alerts incoming voluminous traffic or volumetric attack on IoT devices. These make mitigating DDoS attacks much easier.

Furthermore, since DDoS attacks are implemented in the network layer (Chaganti et al., 2022), I would suggest segmenting the IoT devices from the critical systems. To reduce the impact of unforeseen or potential DDoS attacks. Behavioral anomaly detection can help in the early detection of DDoS attacks.

It is also important that we uphold security in the user/ human approach to mitigating DDoS attacks. To instruct and guide users on how to install necessary configurations and regular/ automatic updates where necessary. Educate users to understand anomaly behavior within the IoT devices and block or report it immediately. Provide security training to the users on security

IOT devices, for example, the smart TV can have an IoT display on essential security training incorporated in smart devices.

ABBREVIATIONS

HTTP:	Hypertext Transfer Protocol
CoAP:	Constrained Application Protocol
DDS:	Data Distribution Service
AMQP:	Advanced Message Queuing Protocol
MQTT:	Message Queuing Telemetry Transport
MQTT-SN:	Message Queuing Telemetry Transport for Sensor Network
XMPP:	Extensible Messaging Presence Protocol
HTTP REST:	Hypertext Transfer Protocol REpresentational State Transfer
MDNS:	Multicast Domain Name System
DNS-SD:	Domain Name System Service Discovery
RPL:	Routing Protocol for Low-Power and Lossy Networks
6LoWPAN:	IPv6 over Low-Power Wireless Personal Area Networks
IPv4/IPv6:	Internet ProtocolV6/ V6
LTE-A:	Long Term Evolution Advanced
EPCglobal:	Electronic Product Code GLOBAL
IEEE 802.15.4:	Institute of Electrical Electronics Engineers

REFERENCE

1. Abhishta, A., van Heeswijk, W., Junger, M., Nieuwenhuis, L.J. and Joosten, R., 2020. Why would we get attacked? An analysis of attacker's aims behind DDoS attacks. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *11*(2), pp.3-22.

2. Abubakar, R., Aldegheishem, A., Majeed, M.F., Mehmood, A., Maryam, H., Alrajeh, N.A., Maple, C. and Jawad, M., 2020. An effective mechanism to mitigate real-time DDoS attacks. *IEEE Access*, *8*, pp.126215-126227.

3. Ali, I., Sabir, S. and Ullah, Z., 2019. Internet of things security, device authentication and access control: a review. *arXiv preprint arXiv:1901.07309*.

4. Alharbi, A., Alotaibi, A., Alghofaili, L., Alsalamah, M., Alwasil, N. and Elkhediri, S., 2022, January. Security in social-media: Awareness of Phishing attacks techniques and countermeasures. In *2022 2nd International Conference on Computing and Information Technology (ICCIT)* (pp. 10-16). IEEE.

5. Ande, R., Adebisi, B., Hammoudeh, M. and Saleem, J., 2020. Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, *54*, p.101728.

6. Araya, J.I.I. and Rifà-Pous, H., 2023. Anomaly-based cyberattacks detection for smart homes: A systematic literature review. *Internet of Things*, p.100792.

7. Bansal, M., Nanda, M. and Husain, M.N., 2021, January. Security and privacy aspects for Internet of Things (IoT). In *2021 6th international conference on inventive computation technologies (ICICT)* (pp. 199-204). IEEE.

8. Bawany, N.Z., Shamsi, J.A. and Salah, K., 2017. DDoS attack detection and mitigation using SDN: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, *42*, pp.425-441.

9. Brooks, R.R., Yu, L., Ozcelik, I., Oakley, J. and Tusing, N., 2021. Distributed denial of service (DDoS): a history. *IEEE Annals of the History of Computing*, *44*(2), pp.44-54.

10. Chaganti, R., Bhushan, B. and Ravi, V., 2022. The role of Blockchain in DDoS attacks mitigation: techniques, open challenges and future directions. *arXiv preprint arXiv:2202.03617*.

11. Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S. and Jin, Y., 2018. Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. *Journal of Hardware and Systems Security*, *2*, pp.97-110. https://doi.org/10.1007/s41635-017-0029-7

12. Doshi, K., Yilmaz, Y. and Uludag, S., 2021. Timely detection and mitigation of stealthy DDoS attacks via IoT networks. *IEEE Transactions on Dependable and Secure Computing*, *18*(5), pp.2164-2176.

13. Fereidouni, H., Fadeitcheva, O. and Zalai, M., 2023. IoT and Man-in-the-Middle Attacks. *arXiv preprint arXiv:2308.02479*.

14. Ghazal, T.M., Afifi, M.A.M. and Kalra, D., 2020. Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. *Solid State Technology*, *63*(1s).

15. Gupta, B.B., Chaudhary, P., Chang, X. and Nedjah, N., 2022. Smart defence against distributed Denial of service attack in IoT networks using supervised learning classifiers. *Computers & Electrical Engineering*, *98*, p.107726.

16. Hassan, M.A., Samara, G. and Fadda, M.A., 2022. IoT Forensic Frameworks (DFIF, IoTDOTS, FSAIoT): A Comprehensive Study. *arXiv preprint arXiv:2203.15705*.Hayat R.F., Aurangzeb, S., Aleem, M., Srivastava, G. and Lin, J.C.W., 2022. ML-DDoS: A

blockchain-based multilevel DDoS mitigation mechanism for IoT environments. *IEEE Transactions on Engineering Management*.

17. Heartfield. E et al., “A taxonomy of cyber-physical threats and impact in the smart home,” Comput. Secure., vol. 78, pp. 398–428, 2018
18. Hu, L., Wen, H., Wu, B., Pan, F., Liao, R.F., Song, H., Tang, J. and Wang, X., 2017. Cooperative jamming for physical layer security enhancement in the Internet of Things. *IEEE Internet of Things Journal*, *5*(1), pp.219-228.
19. Ibrahim, K.L. and Azeez, L.I., 2021, October. Investigate the impact of three wormhole attacks on MANET. In *2021 13th IFIP Wireless and Mobile Networking Conference (WMNC)* (pp. 84-91). IEEE.
20. Karimi, K. and Krit, S., 2019, July. Smart home-smartphone systems: Threats, security requirements and open research challenges. In *2019 International Conference of Computer Science and Renewable Energies (ICCSRE)* (pp. 1-5). IEEE.
21. Kumari, P. and Jain, A.K., 2023. A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security*, p.103096.
22. Kaur, S., Kumar, K., Aggarwal, N. and Singh, G., 2021. A comprehensive survey of DDoS defence solutions in SDN: Taxonomy, research challenges, and future directions. *Computers & Security*, *110*, p.102423.
23. Khoo, B., 2011, October. RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (pp. 709-712). IEEE.
24. Lawal, M.A., Shaikh, R.A. and Hassan, S.R., 2021. A DDoS attack mitigation framework for IoT networks using fog computing. *Procedia Computer Science*, *182*, pp.13-20
25. Liu, H. and Lang, B., 2019. Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences*, *9*(20), p.4396.
26. Marikyan. D, Papagiannidis. P, and Alamanos. E, “A systematic review of the smart home literature: A user perspective,” Technol. Forecast. Soc. Change, vol. 138, no. September 2018, pp. 139–154, 2019
27. Menscher, D., 2020. Exponential growth in DDoS attack volumes. *Google Cloud Blog*

28. MMishra, N. and Pandya, S., 2021. Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, *9*, pp.59353-59377. **DOI:** 10.1109/ACCESS.2021.3073408

29. Mohammadnia, H. and Slimane, S.B., 2020, April. IoT-NETZ: Practical spoofing attack mitigation approach in SDWN network. In *2020 Seventh International Conference on Software Defined Systems (SDS)* (pp. 5-13). IEEE.

30. Ravi, N. and Shalinie, S.M., 2020. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. *IEEE Internet of Things Journal*, *7*(4), pp.3559-3570.

31. Otoum, Y., Liu, D. and Nayak, A., 2022. DL‐IDS: a deep learning–based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies*, *33*(3), p.e3803. **https://doi.org/10.1002/ett.3803**

32. Rahamathullah, U. and Karthikeyan, E., 2021, May. Distributed denial of service attacks prevention, detection and mitigation–A review. In Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021) (p. 16).

33. Safavi, S, Meer . A. M, E. Keneth Joel Melanie, and Z. Shukur, “Cyber Vulnerabilities on Smart Healthcare, Review and Solutions,” Proc. 2018 Cyber Resil. Conf. CRC 2018, pp. 1–5, 2019

34. Sinanović, H. and Mrdovic, S., 2017, September. Analysis of Mirai malicious software. In *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)* (pp. 1-5). IEEE.

35. Sheth, J. and Dezfouli, B., 2019. Enhancing the energy efficiency and timeliness of IoT communication in WiFi networks. *IEEE Internet of Things Journal*, *6*(5), pp.9085-9097.

36. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. and Markakis, E.K., 2020. A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), pp.1191-1221. **DOI:** 10.1109/COMST.2019.2962586

37. Surianarayanan, C. and Chelliah, P.R., 2023. Integration of the Internet of Things and Cloud: Security Challenges and Solutions–A Review. *International Journal of Cloud Applications and Computing (IJCAC)*, *13*(1), pp.1-30.

38. Tushir, B., Dalal, Y., Dezfouli, B. and Liu, Y., 2020. A quantitative study of ddos and e-ddos attacks on wifi smart home devices. *IEEE Internet of Things Journal*, *8*(8), pp.6282-6292.

39. Vishwakarma, R. and Jain, A.K., 2020. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication systems*, *73*(1), pp.3-25.

40. Wazid, M., Das, A.K., Rodrigues, J.J., Shetty, S. and Park, Y., 2019. IoMT malware detection approaches: analysis and research challenges. *IEEE access*, *7*, pp.182459-182476.

41. Yakubu, B.M., Khan, M.I., Khan, A., Jabeen, F. and Jeon, G., 2023. Blockchain-based DDoS attack mitigation protocol for device-to-device interaction in smart home. *Digital Communications and Networks*, *9*(2), pp.383-392

42. Yang, Y., Wu, L., Yin, G., Li, L. and Zhao, H., 2017. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), pp.1250-1258.