Distributed Denial of Service (DDoS) Attacks

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Distributed Denial of Service (DDoS) Attacks

Classification, Attacks, Challenges, and Countermeasures

Brij B. Gupta & Amrita Dahiya

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

First edition published 2021
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

ISBN: 9780367619749 (hbk)
ISBN: 9781003107354 (ebk)

Typeset in Times LT Std
by KnowledgeWorks Global Ltd.

To my parents and family for their constant support during the course of this book

— B. B. Gupta

To my parents, beloved husband, and my mentor for their motivation throughout the journey of writing this book.

— Amrita Dahiya

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Contents

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Preface

Massive technological breakthroughs have pioneered the complexity, scale, and magnitude of DDoS attacks from a very simple Trinoo platform to the Mirai botnet. The days are gone when DDoS attacks were bound to run iterations for vandalism in the small-scale network. Nowadays, DDoS attacks are a major concern for e-companies, as most businesses rely on online access and the Internet for delivering services, since the Internet was developed for applicability and not security. In addition, enormous development in vulnerable and insecure IoT applications, amplification, and reflective techniques has worsened the situation. Progressively, attackers are always driven by large incentives as compared to the legitimate users or defenders. Consequently, the frequency and intensity of the DDoS attacks is rising at an exponential pace resulting in unparalleled levels of damage. There is no denying the fact that researchers have tried to keep the momentum of proposing defensive mechanisms apace with the massive modernisation of attacking techniques. However, we still lack in a comprehensive and robust DDoS defensive mechanism. Thus, it is very important to analyse the recent trends and different DDoS attack mitigation solutions to explore new research directions.

Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges, and Countermeasures provides an overview of the basic concepts of DDoS attacks, its different types, modes of attack, and examines the various countermeasures that have been proposed so far. In this book, we discuss the importance of incentives, liabilities, and cyber insurance in any technical solution and have provided a detailed taxonomy of technical and economical defensive solutions against DDoS attacks. Further, the book covers various issues and challenges encountered by different platforms like cloud computing and IoT in dealing with the DDoS attacks. In addition, we discuss SDN and blockchain as the new emerging solutions to DDoS attacks due to their unique and unparalleled features. Features like decoupling of data and control plane in SDN and decentralisation of blockchain can provide promising solutions in this particular domain. The book emphasises the idea of moving from only technical solutions to a proper blend of technical and economical solutions against DDoS attacks. It also outlines the existing challenges and provides an insight into future research directions.

This book is designed for the readers with an interest in the cybersecurity domain, including researchers who are exploring different dimensions

associated with the DDoS attacks, developers and security professionals who are focusing on developing defensive schemes and applications for detecting or mitigating DDoS attacks, industrialists who are keen of promoting their security measures or their cyber insurance policies and services with new features, and faculty members across different universities.

The book contains six chapters, with each chapter focusing on bringing an understanding and knowledge of DDoS attacks and their taxonomy along with their defensive mechanisms to the readers. The following list provides a detailed overview of the topics covered in each chapter:

Chapter 1: Fundamentals of DDoS attack: Evolution and Challenges – This chapter introduces the concept of DDoS attacks as a starting point for newcomers to the technology and illuminates some major recent trends and statistics unveiled by well-known organisations across the world showcasing the exponential rise in magnitude, severity, and complexity of DDoS attacks. Further, this chapter discusses the evolution of DDoS attacks and their detailed taxonomy based on various parameters.

Chapter 2: Role of Incentives, Liabilities, and Cyber Insurance – This chapter illuminates the importance of incentives and liabilities in any DDoS defensive mechanism. It highlights cyber insurance and its conceptualisation in the risk assessment process. It discusses the fact that weak defense mechanisms, fragile cryptographic protocols, and loose access control policies are not the only reasons, but the lack of incentives and liabilities also contribute significantly to security breaches.

Chapter 3: Taxonomy of DDoS Defence Mechanisms – This chapter highlights the detailed taxonomy of DDoS defense mechanisms. Apart from this, it also covers open research challenges and issues in any trivial DDoS defense mechanism.

Chapter 4: Taxonomy of Economical Solutions – This chapter discusses the classification of economic defensive mechanisms against DDoS attacks. Various payment schemes, resource allocation schemes, negotiation-based solutions, and Internet pricing schemes are discussed in this chapter. Pros and cons of economic solutions are also discussed.

Chapter 5: DDoS Attacks on Various Platforms – This chapter illustrates DDoS attacks on platforms like cloud computing and IoT. It covers vulnerabilities, issues, and challenges associated with these platforms with regard to DDoS attack. Apart from this, this chapter also highlights taxonomy of DDoS attacks and some significant defensive solutions on cloud computing and IoT.

Chapter 6: Emerging Solutions for DDoS attacks: Based on SDN and Blockchain Technologies – This chapter illustrates some new emerging solutions for handling DDoS attacks, i.e., Software Defined Networking (SDN) and blockchain-based solutions. It also covers advantages of these technologies in mitigating DDoS attacks.

Acknowledgements

Writing a book is not a work of an individual, but it is the outcome of the incessant support of our loved ones. This book is the result of the inestimable hard work, continuous efforts, and assistance of loved ones. Therefore, we would like to express our gratefulness to each one of them who are linked with this book, directly or indirectly, for their cooperation and creative ideas for ameliorating the quality of this book. We would also like to express our appreciation for CRC Press, Taylor & Francis Group, editor and staff for their assistance and unfailing support. We are grateful, from the bottom of our hearts, to our family members for their absolute love and countless prayers. This experience has been both internally challenging and rewarding. Therefore, again, special thanks to all who helped us in making this happen. Finally, we would like to express our gratitude to God by bowing our heads for lavishing on us continuous blessings and the enthusiasm to complete this book.

B. B. Gupta
Amrita Dahiya

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

About the Authors

B. B. Gupta received PhD in information and cyber security from Indian Institute of Technology, Roorkee, India. He has published more than 250 research papers in International Journals and Conferences of high repute and has visited several countries like Canada, Japan, the USA, the UK, Malaysia, Australia, Thailand, China, Hong Kong, Italy, Spain, etc. to present his research work. His biography was published in the 30th Edition of *Marquis Who's Who in the World*, 2012. Dr. Gupta also received the Young Faculty Research Fellowship award from the Ministry of Electronics and Information Technology, Government of India, in 2018. He is the principal investigator of various R&D projects. He has served as Associate Editor of IEEE Access, IEEE TII, FGCS, IJICS, IJCSE, ACM TOIT, and ASOC, among other journals. At present, Dr. Gupta is working as an Assistant Professor in the Department of Computer Engineering, National Institute of Technology, Kurukshetra, India. His research interests include Information Security, Cyber Security, Mobile Security, Cloud Computing, Web Security, Intrusion Detection, and Phishing.

Amrita Dahiya is currently pursuing her PhD in cyber security under the supervision of Dr. B. B. Gupta at the Department of Computer Engineering, National Institute of Technology (NIT), Kurukshetra, India. She completed M. Tech at Banasthali University, Rajasthan and her dissertation at Jawaharlal Nehru University, Delhi. Amrita received her B. Tech degree from BRCM College of Engineering and Technology, Bahal in 2012. Her research interests include information and cyber security, Web security, denial of service attacks, online social network, and machine learning. She has published several papers in reputed journals and conferences.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

1 Fundamentals of DDoS Attack: Evolution and Challenges

Substantial development in technology and digitization is constantly extending the world to new milestones and even more difficult challenges. Cutting-edge technologies like Internet of Things (IoT), cloud computing, blockchain, and many other are capable of pushing, enhancing, and automating the lives of people. However, at the same time, these technologies have added fuel to the fire by appending a long list of vulnerabilities and challenges to the existing perils of Internet. People and businesses have constantly been trapped through attacks and threats by attackers [1]. Further, businesses become more dependent on web connectivity for delivery of services, to carry out critical business operations, and to sustain in the market. All these factors contribute immensely to the daunting growth rate of cyberattacks and threats. A Distributed Denial of Service (DDoS) attack is one of the most common types of cyberattacks and has existed since 1974. It still continues to be a major concern for businesses and security professionals. Therefore, this chapter concentrates on comprehensive details of architecture, variants, evolution, and the challenges of DDoS attacks. Further, this chapter covers recent trends and statistics from reliable sources. It will provide readers deep insights into the security threats corresponding to different variants of DDoS attacks.

1.1 DDoS ATTACK: FUNDAMENTALS

A DDoS attack is a massive, distributed, deliberated, and coordinated attack by multiple compromised machines to overwhelm an online service or a server. Attackers attempt to attack the availability of the service by sending voluminous dummy data to make target machine fall short of resources [2]. There exists a huge misalignment of resources as well as of incentives on the Internet, which provides an easy path for attackers to carry out a DDoS attack. A DDoS attack is a variant of Denial of Service (DoS) attack, where the difference lies in the dispersion of attacking source. In DDoS attack, malicious traffic is generated from multiple distributed sources, while in DoS attack, attack is only from a single source [3]. In this attack, the traffic sent by individual bot machines is not huge enough to disrupt the availability of a service, but it is the result of cumulative effect of efforts made by several bot machines. Attackers usually create a network of compromised machines, i.e., botnet by secretly inserting malicious scripts into them. After taking control of the machines, attackers send spam, distribute malware, and tend to attack other systems by exploiting compromised machine. Apart from this method, attackers tend to exploit vulnerabilities of layers 3, 4, and 5 protocols of Open Systems Interconnection (OSI) reference model, which will be discussed later in this chapter. During early days, this attack was only meant to run a certain set of malicious scripts. But technological advancements and constantly increasing incentives have always placed attackers ahead of defenders. The DDoS attack is a significant risk to online businesses, as few minutes of downtime can have serious repercussions like financial or reputational loss [4]. Now, we will discuss the statistics and recent trends, architecture, and types of DDoS attacks.

1.1.1 Statistics and Recent Trends

The established vulnerabilities and the existing botnets have continuously been explored and exploited by the attackers. The moment a new vulnerability is marked, attackers start working on launching a new series of DDoS attacks by exploiting it. The DDoS attack has always been a preferable choice of attackers, as its mitigation is not as easy as its instigation. The largest DDoS attack, of size 1.7 Tbps, was carried out against Github in 2018 (Figure 1.1) [5]. This attack was considered as the largest attack in history until even more disastrous attack of 2019 joined the race. An unnamed client of Imperva had suffered a DDoS attack with a size of 500 million packets per second. Afterwards,

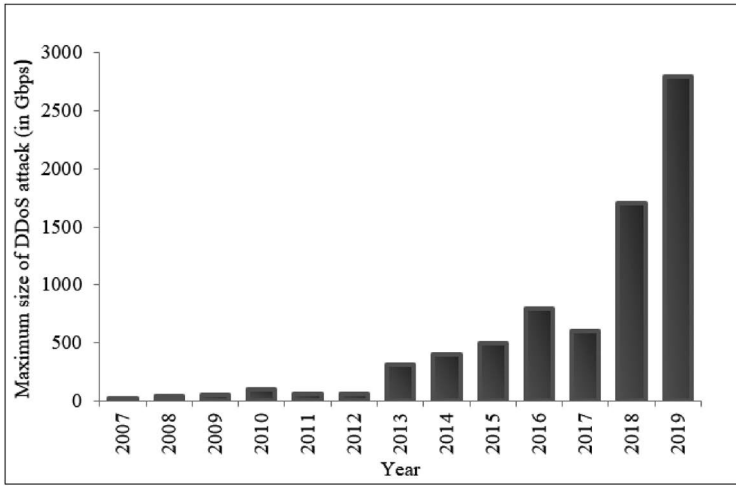

FIGURE 1.1 The largest DDoS attack recorded each year. (Arbour Network Inc.)

the same client had survived an attack with a size of 580 million packets per second in the second quarter of 2019 [6]. Github in 2018 had endured 129.6 million packets per second. Therefore, it can be seen here that in 2019, this attack was almost four times larger than that in 2018.

According to Cisco Visual Networking Index (VNI), by 2022, the number of DDoS attacks will rise up to 14.5 million and may represent 25% of a country's total Internet traffic [7]. Another important trend in this domain is the usage of multi-vector DDoS attack against a single target. In a multi-vector DDoS attack, an attacker tends to merge multiple variants of DDoS attack to not leave any scope for target's survival [8]. Apart from this, another important trend is the usage of "low intensity incursions" that steadily degrade the performance of the target machine over time. These types of attack empower longer attacks that sustain below the threshold value, which can trigger the DDoS defence [44].

In 2019, a company named A10 network had claimed to track approximately 20.3 million DDoS weapons, i.e., infected machines and devices that were available to launch DDoS attack any time [9]. Further, the advent of Internet of Things (IoT) has added fuel to the fire by adding numerous insecure and vulnerable devices to the Internet. These insecure devices are easy to compromise and their abundance has paved a facile path for attackers to create a disastrous botnet. Botnets like Mirai [10], Torii [11], and Daemon bot [12] have proved their fatalness over some past years.

As far as the economic losses are concerned, there is a loss of $12,000 to a small- to medium-sized business due to a single DDoS attack, while it

may reach to $2 million for a big enterprise [13]. Next, the COVID-19 pandemic has shaken the world and has bring healthcare and medical services to their knees. However, attackers are continuously leveraging this situation by increasing frequency, complexity, and size of DDoS attack to manifold. This pandemic has made people dependent on remote workforces to meet their requirements. A sharp increase in DDoS attack has been witnessed during the first and the second quarter of 2020 as compared to those of 2019. Apart from this, the average duration has also increased during this period [14]. In February and March, a series of serious DDoS attacks were launched against the US Department of Health and Human services. SYN flooding has been used excessively to perform DDoS attack during this period. Apart from this, Internet control message protocol (ICMP), Transmission control protocol (TCP), User datagram protocol (UDP) and Hypertext-transfer protocol (HTTP) flooding attacks have also been used by attackers to carry out attacks. Most of the attacks are Linux-based, however there is a slight increase in window-based attacks too. Apart from this, ransom-based DDoS attacks are continued to be troublesome for organisations from last few years [15, 16–18].

Nowadays, organisations tend to focus on automation and virtualisation for the availability of their services. However, it is a matter of concern that security evolution could not have compatibility with technological transformation [19]. There is no denying the fact that vulnerable and insecure devices are constantly increasing exponentially, while there is only a mere effort in securing them. Severity and complexity of DDoS attacks can be imagined well through these recent statistics and trends.

1.1.2 DDoS Attack Evolution

The first ever DDoS attack was carried out in the University of Illinois in 1974 [20]. CERL's PLATO terminals had been used to execute command "ext". This command was developed to enable PLATO to communicate with the other external terminals. However, a student, named Davis Dannis, had executed this command on multiple PLATO terminals when there were no external terminals attached to them, which made 31 systems to crash simultaneously. Later, this command was removed to fix this problem. Further, in 1988, a student, named Robert Tappan Morris, developed a code to measure the size of the Internet [21]. However, this piece of code had the capability to replicate itself and it had destroyed almost 60000 nodes over the Internet. This malicious code was named as Morris worm. The next major attack was carried out in 1999 when a macro virus, named Melissa, spread itself through infected file document attached to an email [22]. This virus had the potential to disseminate to 50 more users from the contact list of the user, who

opened this infected file. This virus had increased the mail traffic all over the world and forced many big companies to shut down their servers. Further, a major DDoS attack was carried out in the University of Minnesota against an Internet Relay Chat (IRC) server through a public interface [23]. It lasted for two days and 227 zombie machines were used to perform this attack. Trinoo was used for the first time to generate UDP flood [24]. It was the year 2000 that witnessed the most destructive DDoS attack ever. A series of DDoS attacks had been launched to some very big companies like Yahoo, eBay, Amazon, and Dell, which caused the damage of approximately 1.2 billion dollars. Afterwards, attacking Domain Name Servers (DNS) became the new trend in 2001 and 2002. In 2002, all 13 root domain name servers of the Internet had been attacked, which created problem for the legitimate users in navigating the Internet.

The above mentioned events are some of the earlier incidents when the DDoS attack has started to evolve, and has continued to sustain as the most disastrous attack till date [25, 26].

1.1.3 Botnet Structure

Attacking techniques are going through a tremendous transformation from attack performed solely to target infrastructure, to hamper national security, and to create nuisance among people. A large number of compromised machines, i.e., botnets are responsible for these disastrous attacks. First, an attacker looks out for vulnerable and insecure host machines and takes control of them by inserting some malicious script [27]. Afterwards, these compromised machines are instructed to direct their traffic towards a specific target. A botnet usually consists of three components, namely, bot master, Command and Control (C&C) channel, and a large number of bots. Bot master controls these bots through C&C channel. Any protocol, for example, HTTP, TCP and UDP can be used to establish C&C between the bot master and the zombies. Now, we will discuss the different botnet architectures (Table 1.1) [28].

TABLE 1.1 Comparison of different types of botnet structures

FEATURES	*ROBUSTNESS*	*EASE OF IMPLEMENTATION*	*EFFICIENCY*
IRC	Low	Simple	Moderate
P2P	High	Complex	High
HTTP	High	Moderate	High

1.1.3.1 Centralised architecture

In this structure, a central management entity is required to communicate with all bot machines. New instructions are given directly by this entity to the bot agents. This architecture was initially used to perform attacks. Bots are easily detectable through this architecture and, therefore, the attack could also be mitigated effectively. It utilises IRC and HTTP for C&C channel. AgoBot, SpyBot, SDBot, and GTBot are some examples of centralised architecture.

1.1.3.2 Peer to peer (P2P) architecture

Attackers focus on peer to peer architecture to overcome the shortcomings of centralised architecture. Though, in this structure, it is difficult for the bot master to control the army of zombies, it is undetectable and cannot be easily blocked by security mechanisms due to the slow consumption of bandwidth at the same time. In this architecture, a compromised peer acts as the bot master as well as a zombie. It disseminates the malicious instructions to other peers in the same way it receives it from others. PhatBot and Peacomm are the examples of peer to peer kind of botnets.

1.1.3.3 Hybrid architecture

It is very similar to peer to peer architecture. However, the only difference is that bot master establishes peer connection only with the supervisor bots. These supervisor bots have their own separate list of zombie machines, which they don't share with other peers for security purposes. Attack from this botnet is difficult to observe and even more difficult to mitigate. This architecture ensures individualised encryption, symmetric traffic dispersal, less exposure to bots, ease of communication with supervisor bots, and strong connectivity among different botnet entities.

1.1.3.4 HTTP2P (HTTP peer to peer) architecture

Peer to peer architecture was designed to overcome the drawbacks of centralised architecture. However, there exists one disadvantage with P2P architecture, i.e., it is prone to sybil attacks. Therefore, attackers have combined HTTP and P2P to make it more robust. In this structure, supervisor bot encrypts the message and looks out for suitable zombie to deliver the message.

1.2 TAXONOMY OF DDoS ATTACKS

A DDoS attack not only has the potential to make target run out of resources but also has the capability to exhaust them on the intermediate networking path. A DDoS attack has a vast taxonomy as it has many variants [29]. We will discuss taxonomy of DDoS attack in this section according to different parameters.

1.2.1 Types of DDoS Attacks

In this category, we have three types of DDoS attacks, namely, voluminous or flooding attack, protocol-based attack, and application layer attack (Table 1.2). Following are its types:

1.2.1.1 Voluminous attack

In this attack, dummy data requests are generated in ample amount from multiple distributed sources and directed towards a specific node. The main motive of an attacker is to deplete the bandwidth of the targeted node. The attacker takes advantage of the fact that the Internet structure is meant for functionality and not for providing security to the users. Further, amplification techniques aid attacker to scale up the size of the attack. Figure 1.4 shows the HTTP flood attack. For example, in reflective DDoS attack, attacker demands usually a large response from the server in return of small service request [30]. This service request would make server to search all its log files and web pages to generate a proper response, which require enormous resources. Smurf attack and UDP storm attack are some of its examples.

1.2.1.2 Protocol-based attack

In the OSI reference model, every layer has a stack of protocols and every protocol exhibits some vulnerabilities and loopholes. In protocol-based attack, the attackers take advantage of these vulnerabilities to perform a DDoS attack [30, 31]. They tend to exploit mainly layers 3 and 4 protocols to exhaust the processing capabilities and memory of the target node. For example, TCP SYN and ping of death attack.

TABLE 1.2 DDoS attack types

ATTACK TYPE	*ATTACK NAME*	*DESCRIPTION*
Voluminous attack	Smurf attack [32]	• ICMP protocol is utilised by network administrators to exchange information about network management and used to check operational status of another device. • An attacker creates a data packet having ICMP message with a spoofed IP address of the victim and then broadcasts it in the network. • Whosoever receives this data packet, will respond to embedded IP packet with a reply which makes victim node flood with ICMP responses.
	UDP storm attack [32]	• Unlike TCP, UDP does not require three-way handshake process to establish connection with the user. • UDP has relatively less overhead in the network and thus effectively used by attackers to perform a UDP flood attack. • "Best effort" data traffic is pushed by attackers through UDP path to overwhelm an online service or machine. • Further, UDP has not any policy for data monitoring or checking, hence this attack is carried out with so much ease and with mere resources.
	DNS amplification attack [33]	• DNS requests are sent with spoofed IP address to DNS server and this would make DNS server to direct all its responses to the target node. • An attacker tends to convert a smaller request into a much larger payload.
	Peer to peer attack [32]	• P2P technology is being widely used for file sharing and downloading and distributed computing. • Unlike conventional botnet, in P2P botnet, an attacker does not communicate with every zombie. • Automated feature of P2P botnet helps in amplifying the attack to a great extent.

Protocol-based attacks	TCP SYN attack [34]	• An attacker sends a connection request to server using SYN flag to which server responds with an acknowledgement using SYN-ACK flag. • A legitimate client would respond to this SYN-ACK packet with an ACK flag. However, a malicious user exploits this feature and does not send this acknowledgement to the server. • Likely, this would end up in exhaustion of memory at server side as there are a large number of half open connections at server. Server tends to wait for ACK until the timer expires.
	Ping of Death (PoD) [35]	• It exploits basic TCP/IP structure of Internet. • Oversized malformed data packets are sent to the victim using ping command. Generally, maximum payload size of a data packet is 84 bytes. It is not allowed to send a data packet larger than this size. Therefore, an attacker breaks a large-sized data packet into fragments and send them to the victim node. • When victim node reassembles all the fragments, the resultant size is larger than 84 bytes resulting into crashing of server or machine.
	Tear drop attack [36]	• Reassembly algorithm and fragment offset field of IP packet are exploited in this attack. • An attacker creates inconsistency in the fragment offset field of a packet and when all the fragments are reassembled at the server, then overlapping of packets occurs resulting into crashing of server.
Application layer attack	HTTP flood [37]	• A well-planned HTTP flood attack does not require techniques like IP spoofing, amplification methods or tampering techniques. This attack is complete in itself to make a server completely paralyse. • Generally, a user utilises HTTP GET and POST command to communicate with the server. GET is used for retaining static content and POST is used for retaining dynamic content on the web. HTTP POST command usually consumes a large number of resources and an attacker takes advantage of this fact. • It is slow rate attack, and therefore, is difficult to detect.
	Slowloris attack [37]	• Similar to HTTP flood attack, it is also a slow rate attack and sends incomplete information to the server. It makes server to wait indefinitely for the complete information. In other words, an attacker sends HTTP GET request without termination code. • It slowly exhausts the connection capability of server.

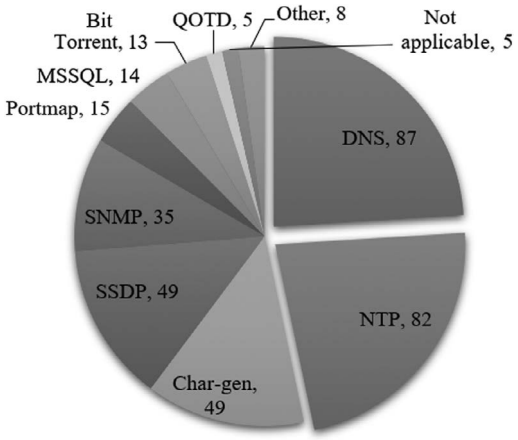

FIGURE 1.2 Targets of application layer attack. (Arbour Network Inc.)

1.2.1.3 Application layer attack

This attack targets the seventh layer of the OSI reference model by obfuscating the web applications (Figure 1.2). This attack is relatively more destructive than the other two types of attacks as it has the capability to ingest network and server resources at the same time. Application layer attacks are the most persistent attacks nowadays. Figure 1.3 shows the different types of protocols exploited by attackers to perform flooding DDoS attack. Figure 1.4 shows the working of HTTP flood attack.

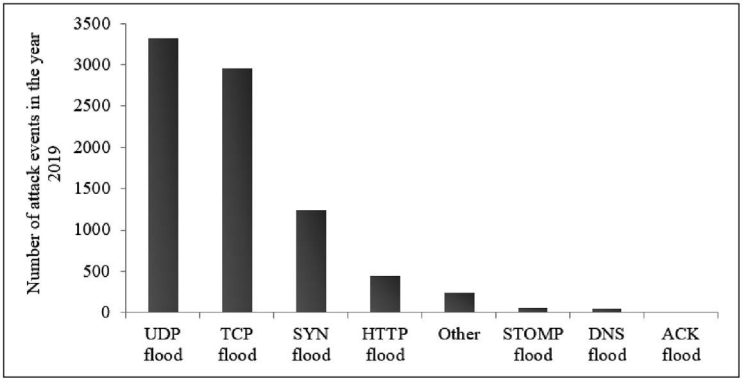

FIGURE 1.3 Types of protocols exploited for flooding DDoS attack.

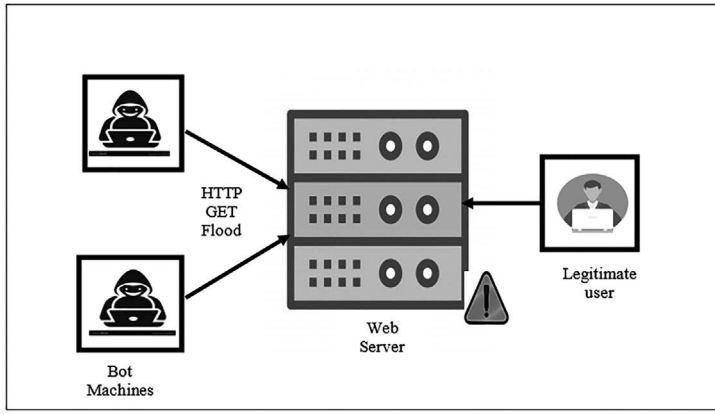

FIGURE 1.4 HTTP flood attack.

1.2.2 Classification Based on Degree of Automation

DDoS attacks can be classified into three categories based on the degree of automation, namely, manual, semiautomatic, and automatic [3], which are discussed below:

1.2.2.1 Manual attack

All phases of the DDoS attack are performed manually in this attack. This method was used during early days, but nowadays, it has become obsolete.

1.2.2.2 Semiautomatic attack

In this type of attack, agent-handler and master-slave botnet architectures are used. An attacker tends to find out the vulnerable systems using automated scanning scripts, and then, malicious codes are inserted into these systems. Further, the attacker instructs these bots to target a specific node through handlers or masters. This attack further falls into categories, namely, direct and indirect attack based on the type of connection between the handlers. In direct semiautomatic attack, an attacker has to embed the IP address of the machine into the malicious code to transform it into a bot. At the moment of attack, in response to the malicious code, the agent has to mark its presence to

the handler by showing its availability. The handler has to keep the list of all agents attached to it, which is a major shortcoming of this structure as revelation of one bot can expose all botnets. In indirect semiautomatic attack, an attacker has to rely on some reliable communication protocols between the handlers to avoid the detectability of the botnet for longer duration.

1.2.2.3 Automatic attack

In automatic attack, unlike manual and semiautomatic attacks, all phases of DDoS attack are carried out without any intervention of an attacker. Malicious code programmed with relevant information regarding attack is used to infect the machines.

1.2.3 Classification Based on Vulnerability Exploited

Weaknesses of the system, protocol, and network have always been exploited by the attackers to perform different variants of DDoS attacks. Following is the classification:

1.2.3.1 Volumetric attack

A large number of dummy data requests are forwarded towards the victim to deplete its bandwidth. Please refer section 1.2.1 for detailed information of this attack.

1.2.3.2 Amplification attack

In this attack, the broadcasting feature of an IP network is exploited to scale up size and frequency of a DDoS attack. An attacker tries to generate a small service request, but ensures that the response must have a larger payload size resulting in the exhaustion of resources at server side. DNS amplification and Smurf attacks are the examples of amplification attack, which have already been discussed.

1.2.3.3 Deformed packet attack

In this attack, the IP header of the data packet is falsified or tampered and, then, forwarded to the victim node. Tear drop and ping of death are the examples of deformed packet attack.

1.2.3.4 Protocol-based attack

In this attack, vulnerabilities of layers 3 and 4 are exploited to target processing capability and memory of the target node. Please refer section 1.2.1.2 for detailed information.

1.2.4 Classification Based on Attack Rate

The DDoS attacks can be classified into following three categories based on the attack rate:

1.2.4.1 High rate attack

In this attack, the attacker aims to make online service completely unavailable for longer duration for legitimate users. It is the most destructive than other two attacks.

1.2.4.2 Variable rate attack

In this attack, the attacker varies his rate of sending malicious traffic according to the response generated by the victim machine.

1.2.4.3 Low rate attack

This attack aims to slowly degrade the Quality of Service (QoS) of an online service for legitimate users. This attack sustains for longer duration as it is difficult to detect.

1.3 ATTACK TOOLS

There exist many freely available DDoS attacking tools online. An attacker with naïve knowledge and slight modifications can carry out a DDoS attack with the help of these tools. Table 1.3 lists some of the important attacking tools.

TABLE 1.3 DDoS attack tools

ATTACK TOOL	*DESCRIPTION*	*ATTACK*
Mstream [38]	• Counterfeit TCP packets are utilised with ACK flag to perform an attack. • Bandwidth exhaustion attack tool. • Master/slave architecture is employed. • It sends spoofed TCP SYN packet to different servers and broadcasting networks. These servers and broadcasting networks send ACK packets directed towards victim network in response to TCP SYN packets.	TCP ACK
Trinoo [39]	• Bandwidth debilitation tool. • Master-slave botnet is employed to carry out attack against multiple hosts. • IP spoofing is not used by this tool.	UDPfFlooding
HOIC [40]	• Improved version of LOIC. • It can attack 256 targets simultaneously. • Generates ample amount of HTTP GET and POST requests towards application server. • Manual intervention is required for coordination among attackers. • Attacker can easily be traced back.	HTTP flooding attack
XOIC [41]	• More destructive than LOIC. • IP address, port number, or type of protocol need to be specified by the attacker. • Easy tool for naïve users. • Attacker can easily be traced back.	HTTP, UDP, TCP and ICMP flooding attack.
LOIC [42]	• It can perform URL and IP address-based attack. • Attacker's IP address cannot be hidden. • IRC help other users to join in middle of the attack.	HTTP, TCP, UDP flooding attack

Tribe Flood Network [39]	• There is no encryption between handler and attacker or agent and handler. • Command line argument is used to instruct handlers. • It can deplete bandwidth and other resources at target.	TCP SYN, UDP flooding, ICMP. Smurf attack
PyLoris	• Testing tool for servers. • SOCKS proxies and SSL connections are utilised to perform DoS attack. • Various protocols like FTP, SMTP, HTTP, Telnet, and IMPAP can be attacked easily. • Written in Python. • Open TCP connections for as much long as possible.	PyLoris
HULK	• Obfuscated traffic is generated to bypass a caching engine. • Attack detection can be avoided. • Different fields of a web request can be forged easily. • Traffic from HULK can be blocked.	HTTP flooding attack.
Stacheldraht [39]	• Features of Tribe Flood Network and Trinoo are combined with encryption as the added feature. • Uses agent handler architecture. ICMP is used for communication between agent and handler, while TCP is used for communication between client and handler.	ICMP and UDP flooding attack, Smurf attack, TCP SYN attack.
Knight [43]	• IRC-based, a strong attacking tool. • A Trojan Horse program, named back Orifice, is used to compromise a system. • It has a checksum generator.	TCP and UDP Flooding attack. TCP SYN attack.
DDoSim	• All compromised systems create full TCP connection with the victim server. • It generates legitimate HTTP requests to flood the victim.	HTTP and TCP flooding attack.

1.4 CHAPTER SUMMARY

Every business domain has some form of dependency, i.e., direct or indirect on the Internet. This dependency has exposed businesses to various types of cyberattacks and threats. A DDoS attack is one of the cyberattacks, which involves direct implication of Internet structure and uneven distribution of resources over it. This attack is considered as the most generic attack in the sense that it can be carried out at any point in the network. This attack is not peculiar about certain networking requirements. Therefore, it is still continued to be a matter of concern for the whole research community. Hence, the focus of this chapter is to elaborate the DDoS attack, its history, evolution, botnet architecture, and taxonomy. Further, this chapter also contains recent statistics and trends unveiled by some security organisations. Moreover, this chapter also illuminates different variants of DDoS attacks along with widely used attacking tools.

REFERENCES

1. E. Fenil and P. Mohan Kumar, "Survey on DDoS defense mechanisms," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 4, p. e5114, 2020.
2. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 303–336, 2013.
3. S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.
4. D. Chaudhary, K. Bhushan, and B. B. Gupta, "Survey on DDoS attacks and defense mechanisms in cloud and fog computing," *International Journal of E-Services and Mobile Applications (IJESMA)*, vol. 10, no. 3, pp. 61–83, 2018.
5. Skottler, "February 28th DDoS Incident Report." 2018.
6. Tomer Shani, "Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important," 2019.
7. Cisco Visual Networking Index (VNI), "Cisco Predicts More IP Traffic in the Next Five Years Than in the History of the Internet", November 27, 2018. Link available: https://newsroom.cisco.com/press-releasecontent?type=webcontent&articleId=1955935.
8. Marek Majkowski, "The rise of multivector DDoS attacks", The CloudFlare Blog. Link available: https://blog.cloudflare.com/the-rise-of-multivector-amplifications/.

9. A10 networks, "A10 Networks DDoS Threat Intelligence Finds IoT Devices a Growing Part of Global DDoS Weapon Arsenal", SAN JOSE, Calif., March 5, 2019. Link available at: https://www.a10networks.com/news/press-releases/a10-networks-ddos-threat-intelligence-finds-iot-devices-growing-part-of-global-ddos-weapon-arsenals/.
10. J. Fruhlinger, "The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet," India, 2018.
11. Neduchal, Jan, Hron, Martin, Kroustek, Jakub, Iliushin, Vladislav, and Shirokova, Anna (2018), Torii botnet - Not Another Mirai Variant.
12. Georg Wicherski, Markus Kötter, Paul Bächer, Thorsten Holz (2005). "Know your enemy: Tracking Botnets". The Honeynet Project & Research Alliance, pp. 1–17.
13. Kobialka Dan, "Kaspersky Lab Study: Average Cost of Enterprise DDoS Attack Totals $2M.", February 25, 2018. Link available at: https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/.
14. Radware, "Smart DDoS Protection During the COVID-19 Crisis", August 4, 2020. Link available at: https://blog.radware.com/security/ddos/2020/08/smart-ddos-protection-during-the-covid-19-crisis/.
15. Kaspersky, "KSN Report: Ransomware in 2016–2017," 2017.
16. R. A. Esraa Alomari, Selvakumar Manickam, et al.,"Botnet-based distributed denial of service (DDoS) attacks on web servers: Classification and art." *International Journal of Computer Application (IJCA)*, vol. 49, no. 7, pp. 24–32, 2012.
17. K. Bhushan and B. B. Gupta, "Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment." *Journal of Ambient Intelligence and Humanized Computing, Springer*, vol. 10, no. 5, pp. 1985–1997, 2019.
18. Gupta, B. B. (2011). An Introduction to DDoS Attacks and Defense Mechanisms: An Analyst's Handbook. Lap Lambert Academic Pub. Germany.
19. Gupta, B. B., Dahiya, A., Upneja, C., Garg, A., and Choudhary, R. (2020). "A comprehensive survey on DDoS attacks and recent defense mechanisms." In Handbook of Research on Intrusion Detection Systems (pp. 186–218). IGI Global.
20. Radware, "History of DDoS Attacks," 2017.
21. S. Malenkovich, "Morris Worm Turns 25," 2013.
22. Nota Bene, "A Brief History of DDoS Attacks," 2016.
23. Lee Garber, "Denial-of-Service Attacks Rip the Internet," *Computer (Long. Beach. Calif).*, vol. 33, no. 4, pp. 12–17, 2000, doi: 10.1109/MC.2000.839316.
24. D. Dittrich, "The DoS Project's 'trinoo'distributed denial of service attack tool," 1999.
25. Badve, Omkar P., Shingo Yamaguchi, and Zhaolong Gou, et al., "DDoS detection and filtering technique in cloud environment using GARCH model." In 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), pp. 584–586. IEEE, 2015.
26. Agrawal, P. K., B. B. Gupta, Satbir Jain, and M. K. Pattanshetti. "Estimating strength of a DDoS attack in real time using ANN based scheme." In International Conference on Information Processing, pp. 301–310. Springer, Berlin, Heidelberg, 2011.

27. R. Puri, "Bots and Botnet: An Overview," Technical Report, SANS Institute, 2003.
28. B. Al-Duwairi, and M. Jarrah, "Botnet architectures." *Botnets: Architectures, Countermeasures, and Challenges*, vol.1, 2019.
29. B. B. Gupta, and O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment." *Neural Computing and Applications*, vol. 28, no. 12, pp. 3655–3682, 2017.
30. K. Sharma, and B. B. Gupta, "Taxonomy of distributed denial of service (DDoS) attacks and defense mechanisms in present era of smartphone devices." *International Journal of E-Services and Mobile Applications (IJESMA)*, vol. 10, no. 2, pp. 58–74, 2018.
31. Patel, S., Patel, D., and Nazir, S. (2020). Cloud-based Autonomic Computing Framework for Securing SCADA Systems. IGI Global.
32. Lau, F. , S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks." In IEEE International Conference on Systems, Man, and Cybernetics, Nashville, TN, vol. 3, p. 2275–2280, IEEE, 2000.
33. Rossow, Christian. (2014). Amplification Hell: Revisiting Network Protocols for DDoS Abuse. NDSS.
34. CERT Advisory CA-1996-21, Carnegie Mellon University, 2014, https://www.uxsup.csx.cam.ac.uk/pub/webmirrors/www.cert.org/advisories/CA-1996-21.html.
35. Ping of Death, 2019, Cloudflare blog [Online]. Available from: https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/.
36. CERT Advisory CA-1997-28, Carnegie Mellon University, 2014, https://resources.sei.cmu.edu/asset_files/whitepaper/1997_019_001_496176.pdf.
37. C. Enrico et al. "Slow DoS attacks: Definition and categorisation." *International Journal Trust Management Computer Communication*, vol. 1, pp. 300–319, 2013.
38. D. Dittrich, G. Weaver, S. Dietrich, and N. Long, "The 'mstream' distributed Denial of Service Attack Tool." Technical Report. University of Washington, Seattle, USA, 2000, https://staff.washington.edu/dittrich/misc/mstream.analysis.txt.
39. D. Dittrich, "The DoS project's ''trinoo'' distributed denial of service attack tool," 1999, https://staff.washington.edu/dittrich/misc/trinoo.analysis.
40. HOIC, Sourceforge.net, 2019, http://sourceforge.net/projects/hoic/.
41. XOIC, Sourceforge.net, 2019, http://sourceforge.net/projects/xoic/.
42. LOIC, Sourceforge.net, 2019, http://sourceforge.net/projects/loic/.
43. B.B. King, and D. Morda, "CERT Coordination Centre, CERT Advisory CA-2001–20 Continuing Threats to Home Users." Technical Report, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA, 2001, https://seclists.org/cert/2001/14.
44. Conran Matt, "The rise of artificial intelligence DDoS attacks," 2018.

REFERENCES

1. Wu, Wu, Y., Fung, R. Y., Feng, G., & Wang, N. (2017). Decisions making in information security outsourcing: Impact of complementary and substitutable firms. *Computers & Industrial Engineering, 110*, 1–12.
2. Kumar, A. (2019). Design of secure image fusion technique using cloud for privacy-preserving and copyright protection. *International Journal of Cloud Applications and Computing (IJCAC)*, *9*(3), 22–36.
3. Anderson, Ross, & Moore, Tyler. (2006). The economics of information security. *Science, 314*(5799), 610–613.
4. Gupta, Brij B., Ramesh C. Joshi, and Manoj Misra. "An efficient analytical solution to thwart DDoS attacks in public domain." In *Proceedings of the international conference on advances in computing, communication and control*, pp. 503–509. 2009.
5. Agrawal, P. K., Satbir Jain, and M. K. Pattanshetti, et al., (2011). "Estimating strength of a DDoS attack in real time using ANN based scheme." In *International Conference on Information Processing*, pp. 301–310. Springer, Berlin, Heidelberg.
6. Gupta, Brij B. (2012). Predicting number of zombies in DDoS attacks using pace regression model. *Journal of Computing and Information Technology, 20*(1), 33–39.
7. Geng, X., & Whinston, A. B. (2000). Defeating distributed denial of service attacks. *IEEE IT Professional*, *2*, 36–41.
8. Naraine, R. (2002). Massive DDoS attack hit DNS root servers.
9. Luong, N. C., Hoang, D. T., Wang, P., Niyato, D., Kim, D. I., & Han, Z. (2016). Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey. *IEEE Communications Surveys & Tutorials*, *18*(4), 2546–2590.
10. Dahiya, A., & Gupta, B. B. (2020). Multi attribute auction based incentivized solution against DDoS attacks. *Computers & Security*, *92*, 101763.
11. Gupta, B. B., & Sheng, Q. Z. (Eds.). (2019). *Machine learning for computer and cyber security: Principle, algorithms, and practices*. CRC Press, Boca Raton, FL.
12. Gupta, Brij, Agrawal, Dharma P., &Yamaguchi, Shingo. (Eds.). (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI global.
13. Adat, Vipindev, Amrita Dahiya, et al., "Economic incentive based solution against distributed denial of service attacks for IoT customers." In 2018 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–5. IEEE, 2018.
14. Gordon, Lawrence A., & Loeb, Martin P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438–457.

15. Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: The mediation role of risk perception. *IEEE Access*, *7*, 111341–111354.
16. Anderson, Ross. "Why cryptosystems fail." *Proceedings of the 1st ACM Conference on Computer and Communications Security*. ACM, 1993.
17. Kenneally, E. (2019). Economics and incentives driving IoT privacy and security, Pt. 1. *IEEE Internet of Things Magazine, 2*(1), 6–7.
18. Tilting the playing field: How misaligned incentives work against cybersecurity by Mcafee. Link available at: https://www.csis.org/events/tilting-playing-field-how-misaligned-incentives-work-against-cybersecurity.
19. Kathleen Metrick, Jared Semrau, & Shambavi Sadayappan, "Think fast: Time between disclosure, patch release and vulnerability exploitation — Intelligence for vulnerability management, part two," April 30, 2020, Fireeye Blogs.
20. Smith, M. W. (2019). Information asymmetry meets data security: The lemons market for smartphone apps. *Policy Perspectives*, 85–96.
21. Zhang, R., & Zhu, Q. (2019). A game-theoretic cyber insurance framework for incentive-compatible cyber risk management of Internet of Things. *IEEE Transactions on Information Forensics and Security*, *15*, 2026–2041.
22. Wang, J., & Wang, C. (2018). Full secure identity-based encryption scheme over lattices for wireless sensor networks in the standard model. *International Journal of High Performance Computing and Networking*, *12*(2), 111–117.
23. de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7.
24. Woods, D. W., & Moore, T. (2019). Does insurance have a future in governing cybersecurity? *IEEE Security & Privacy*, *18*(1), 21–27.
25. Vagle, J. L. (2020). Cybersecurity and Moral Hazard. *Stan. Tech. L. Rev.*, *23*, 71.
26. Mishra, N. (2020). The Trade: (Cyber) security dilemma and its impact on global cybersecurity governance. *Journal of World Trade*, *54*(4).
27. Xu, Y., D. Tran, Y. Tian, and H. Alemzadeh. "Analysis of cyber-security vulnerabilities of interconnected medical devices." In 2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), pp. 23–24. IEEE, 2019, September.
28. Anderson, R. (2002). Security in open versus closed systems—The dance of Boltzmann, Coase and Moore. Technical report, Cambridge University, England.

29. Ozment, Andy. (2005, June 2–3) The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting, Fourth Workshop on the Economics of Information Security, Cambridge, MA.
30. Versen, M., & Ernst, W. (2020). Row hammer avoidance analysis of DDR3 SDRAM. *Microelectronics Reliability*, 113744.
31. Carfora, M. F., Martinelli, F., Mercaldo, F., & Orlando, A. (2019). Cyber risk management: An actuarial point of view. *Journal of Operational Risk*, *14*(4), 77–103.
32. Russo, P., Caponi, A., Leuti, M., & Bianchi, G. (2019). A web platform for integrated vulnerability assessment and cyber risk management. *Information*, *10*(7), 242.
33. Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1), tyz002.
34. Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers*, *21*(5), 997–1018.
35. Khalili, M. M., Liu, M., & Romanosky, S. (2019). Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Journal of Cybersecurity*, *5*(1), tyz010.
36. Liu, M. (2019). *A new paradigm in risk-informed cyber insurance policy design: Meta-policies and risk aggregation*. Regents of the University of Michigan Ann Arbor United States Ann Arbor, MI.
37. Singh, O., & Singh, M. (2020). A Comparative Analysis on Economic Load Dispatch Problem Using Soft Computing Techniques. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, *12*(2), 50–73.
38. Gavėnaitė-Sirvydienė, J. (2019). Evaluation of Cyber Insurance as a Risk Management Tool Providing Cyber-Security.
39. Nurse, Jason R. C., Axon, Louise, Erola, Arnau, Agrafiotis, Ioannis, Goldsmith, Michael, Creese, Sadie (2020) The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. In: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE (doi:10.1109/CyberSA49311.2020.9139703) (KAR id:80965)
40. Bhattacharya, P., & Guo, M. (2020). An Incentive Compatible Mechanism for Replica Placement in Peer-Assisted Content Distribution. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, *12*(1), 47–67.
1. K. Bhushan and B. B. Gupta, "Security challenges in cloud computing: state-of-art," *International Journal of Big Data Intelligence*, vol. 4, no. 2, pp. 81–107, 2017.

2. P. Sharma, J. Sengupta, and P. K. Suri, "Survey of intrusion detection techniques and architectures in cloud computing," *International Journal of High Performance Computing and Networking*, vol. 13, no. 2, pp. 184–198, 2019.
3. B. B. Gupta, S. Gupta, and P. Chaudhary, "Enhancing the browser-side context-aware sanitization of suspicious HTML5 code for halting the DOM-based XSS vulnerabilities in cloud," *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 7, no. 1, pp. 1–31, 2017.
4. J. K. Chahal, A. Bhandari, and S. Behal, "Distributed denial of service attacks: A threat or challenge," *New Review of Information Networking*, vol. 24, no. 1, pp. 31–103, 2019.
5. B. B. Gupta, D. P. Agrawal, S. Yamaguchi, and M. Sheng, "Advances in applying soft computing techniques for big data and cloud computing," 2018.
6. O. Singh and M. Singh, "A comparative analysis on economic load dispatch problem using soft computing techniques," *International Journal of Software Science and Computational Intelligence (IJSSCI)*, vol. 12, no. 2, pp. 50–73, 2020.
7. Y. Li, L. Guo, Z.-H. Tian, and T.-B. Lu, "A lightweight web server anomaly detection method based on transductive scheme and genetic algorithms," *Comput. Commun.*, vol. 31, no. 17, pp. 4018–4025, 2008.
8. A. Rahul, S. K. Prashanth, B. Suresh Kumar, and G. Arun, "Detection of intruders and flooding in VoIP using IDS, Jacobson fast and Hellinger distance algorithms," *IOSR J. Comput. Eng.*, vol. 2, no. 2, pp. 30–36, 2012.
9. W. Wei, Y. Dong, D. Lu, and G. Jin, "Combining cross-correlation and fuzzy classification to detect distributed denial-of-service attacks," in International Conference on Computational Science, 2006, pp. 57–64.
10. J. M. Gonzalez, M. Anwar, and J. B. D. Joshi, "A trust-based approach against IP-spoofing attacks," in 2011 Ninth Annual International Conference on Privacy, Security and Trust, 2011, pp. 63–70.
11. S. N. Shiaeles, V. Katos, A. S. Karakos, and B. K. Papadopoulos, "Real time DDoS detection using fuzzy estimators," *Comput. Secur.*, vol. 31, no. 6, pp. 782–790, 2012.
12. J. Wang and G. Yang, "An intelligent method for real-time detection of DDoS attack based on fuzzy logic," *J. Electron.*, vol. 25, no. 4, pp. 511–518, 2008.
13. S. M. Lee, D. S. Kim, J. H. Lee, and J. S. Park, "Detection of DDoS attacks using optimized traffic matrix," *Comput. Math. with Appl.*, vol. 63, no. 2, pp. 501–510, 2012.
14. R. Vijayasarathy, S. V. Raghavan, and B. Ravindran, "A system approach to network modeling for DDoS detection using a Naive Bayesian classifier," in 2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011), 2011, pp. 1–10.

15. W. Haider, N. Moustafa, M. Keshk, A. Fernandez, K. K. R. Choo, and A. Wahab, "FGMC-HADS: Fuzzy Gaussian mixture-based correntropy models for detecting zero-day attacks from Linux systems," *Computers & Security*, 101906, 2020.
16. S. Velliangiri and H. M. Pandey, "Fuzzy-Taylor-elephant herd optimization inspired deep belief network for DDoS attack detection and comparison with state-of-the-arts algorithms," *Future Generation Computer Systems*, vol. 110, pp. 80–90, 2020.
17. C.-M. Cheng, H. T. Kung, and K.-S. Tan, "Use of spectral analysis in defense against DoS attacks," in Global Telecommunications Conference, 2002. GLOBECOM'02*, IEEE,* 2002, vol. 3, pp. 2143–2148.
18. J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," in 10th IEEE International Conference on Network Protocols, 2002, Proceedings, 2002, pp. 312–321.
19. G. Zhang, S. Jiang, G. Wei, and Q. Guan, "A prediction-based detection algorithm against distributed denial-of-service attacks," in Proceedings of the 2009 international conference on wireless communications and mobile computing: Connecting the World wirelessly, 2009, pp. 106–110.
20. J. Cheng, J. Yin, C. Wu, B. Zhang, and Y. Liu, "DDoS attack detection method based on linear prediction model," in International Conference on Intelligent Computing, 2009, pp. 1004–1013.
21. T. Peng, C. Leckie, and K. Ramamohanarao, "Proactively detecting distributed denial of service attacks using source IP address monitoring," in International conference on research in networking, 2004, pp. 771–782.
22. J. Udhayan and T. Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks," *IJ Netw. Secur.*, vol. 13, no. 3, pp. 152–160, 2011.
23. G. Öke and G. Loukas, "A denial of service detector based on maximum likelihood detection and the random neural network," *Comput. J.*, vol. 50, no. 6, pp. 717–727, 2007
24. Y. Chen, K. Hwang, and W.-S. Ku, "Distributed change-point detection of DDoS attacks over multiple network domains," in Int. Symp. on Collaborative Technologies and Systems, 2006, pp. 543–550.
25. A. Dainotti, A. Pescapé, and G. Ventre, "A cascade architecture for DoS attacks detection based on the wavelet transform," *J. Comput. Secur.*, vol. 17, no. 6, pp. 945–968, 2009
26. K. Kalkan, L. Altay, G. Gür, and F. Alagöz, 2018 "JESS: Joint entropy-based DDoS defense scheme in SDN," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2358–2372.
27. Gupta, B. B. (Ed.). (2018). Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives. CRC Press.
28. Gupta, B. B., Perez, G. M., Agrawal, D. P., & Gupta, D. (2020). Handbook of Computer Networks and Cyber Security. Springer Science and Business Media LLC.

29. Gupta, B. B., and Sheng, Quan Z. (Eds.). (2019). Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices. CRC Press.
30. B. Gupta and M. Chhabra, "A novel solution to handle DDOS attack in MANET," *Journal of Information Security*, vol. 4, no. 3, pp. 165–179, 2013.
31. R. Zhong and G. Yue, "DDoS detection system based on data mining," in Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2010, pp. 2–4.
32. L. Li and G. Lee, "DDoS attack detection and wavelets," *Telecommun. Syst.*, vol. 28, no. 3–4, pp. 435–451, 2005.
33. J. Seo, C. Lee, T. Shon, K.-H. Cho, and J. Moon, "A new DDoS detection model using multiple SVMs and TRA," in International Conference on Embedded and Ubiquitous Computing, 2005, pp. 976–985.
34. K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," *Expert Syst. Appl.*, vol. 34, no. 3, pp. 1659–1665, 2008.
35. J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," *Comput. Commun.*, vol. 31, no. 17, pp. 4212–4219, 2008.
36. K. Hwang, P. Dave, and S. Tanachaiwiwat, "NetShield: Protocol anomaly detection with datamining against DDoS attacks," in Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, 2003, pp. 8–10.
37. H. Rahmani, N. Sahli, and F. Kammoun, "Joint entropy analysis model for DDoS attack detection," in 2009 Fifth International Conference on Information Assurance and Security, 2009, vol. 2, pp. 267–271.
38. R. Thomas, B. Mark, T. Johnson, and J. Croall, "NetBouncer: client-legitimacy-based high-performance DDoS filtering," in Proceedings DARPA Information Survivability Conference and Exposition, 2003, vol. 1, pp. 14–25.
39. L. Limwiwatkul and A. Rungsawang, "Distributed denial of service detection using TCP/IP header and traffic measurement analysis," in *Proc. IEEE Int. Symp. Communications and Information Technology*, Sapporo, Japan, 2004, October 26–29, pp. 605–610.
40. J. Wang, R. C.-W. Phan, J. N. Whitley, and D. J. Parish, "Augmented attack tree modeling of distributed denial of services and tree based attack detection method," in 2010 10th IEEE International Conference on Computer and Information Technology, 2010, pp. 1009–1014.
41. T. M. Gil and M. Poletto, "MULTOPS: A Data-Structure for Bandwidth Attack Detection," in USENIX Security Symposium, 2001, pp. 23–38.
42. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," *Comput. Networks*, vol. 51, no. 18, pp. 5036–5056, 2007.
43. Z. Guangsen, M. Parashar, and others, "Cooperative defence against DDoS attacks," *J. Res. Pract. Inf. Technol.*, vol. 38, no. 1, p. 69, 2006.

44. S. Kent and R. Atkinson, “Security architecture for the internet protocol,” RFC 2401, November, 1998.
45. S. Kent and R. Atkinson, “IP authentication header,” RFC 2402, November, 1998.
46. P. Ferguson and D. Senie, “ Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing,” RFC 2827, 2000.
47. S. Abdelsayed, D. Glimsholt, C. Leckie, S. Ryan, and S. Shami, “An efficient filter for denial-of-service bandwidth attacks,” in GLOBECOM’03. IEEE Global Telecommunications Conference (IEEE Cat. No. 03CH37489), 2003, vol. 3, pp. 1353–1357.
48. A. John and T. Sivakumar, “Ddos: Survey of traceback methods,” *Int. J. Recent Trends Eng.*, vol. 1, no. 2, p. 241, 2009.
49. R. Chen, J.-M. Park, and R. Marchany, “NISp1-05: RIM: Router interface marking for IP traceback,” in IEEE Globecom 2006, 2006, pp. 1–5.
50. B. Al-Duwairi and M. Govindarasu, “Novel hybrid schemes employing packet marking and logging for IP traceback,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 17, no. 5, pp. 403–418, 2006.
51. L. Cheng, D. M. Divakaran, W. Y. Lim, & V. Thing, U.S. Patent Application No. 16/087,625, 2019.
52. S. Suresh and N. Sankar Ram, “Enhanced deterministic packet marking mechanism for improving performance in scalability when identify attack source,” *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 5–6, pp. 1956–1960, 2019.
53. O. W. Salami, I. J. Umoh, E. A. Adedokun, and M. B. Muazu, “Implementing flash event discrimination in IP traceback using shark smell optimisation algorithm,” *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, vol. 4, no. 3, pp. 259–268, 2019.
54. J. B. D. Cabrera et al., “Proactive detection of distributed denial of service attacks using mib traffic variables-a feasibility study,” in 2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No. 01EX470), 2001, pp. 609–622.
55. S. Suresh and N. S. Ram, “Feasible ddos attack source traceback scheme by deterministic multiple packet marking mechanism,” *The Journal of Supercomputing*, vol. 76, no. 6, pp. 4232–4246, 2020.
56. P. Fazio, M. Tropea, M. Voznak, and F. De Rango, “On packet marking and Markov modeling for IP Traceback: A deep probabilistic and stochastic analysis,” *Computer Networks*, 107464, 2020.
57. Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, “Packetscore: Statistics-based overload control against distributed denial-of-service attacks,” in IEEE INFOCOM *2004*, 2004, vol. 4, pp. 2594–2604.

58. Shah, S. B. I., Anbar, M., Al-Ani, A., & Al-Ani, A. K. (2019). "Hybridizing entropy-based mechanism with adaptive threshold algorithm to detect RA flooding attack in ipv6 networks," in Computational Science and Technology (pp. 315–323). Springer, Singapore.
59. A. T. Mizrak, S. Savage, and K. Marzullo, "Detecting compromised routers via packet forwarding behavior," *IEEE Netw.*, vol. 22, no. 2, pp. 34–39, 2008.
60. L. Zhou, H. Guo, and G. Deng, "A fog computing-based approach to DDoS mitigation in IIoT systems," *Computers & Security*, vol. 85, pp. 51–62, 2019.
61. C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, "Cossack: Coordinated suppression of simultaneous attacks," in Proceedings DARPA Information Survivability Conference and Exposition, 2003, vol. 1, pp. 2–13.
62. Gulihar, P.and Gupta, B. B. (2020). "Cooperative Mechanisms for Defending Distributed Denial of Service (DDoS) Attacks," in Handbook of Computer Networks and Cyber Security (pp. 421–443). Springer, Cham.
63. W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," *Future Generation Computer Systems*, vol. 96, pp. 481–489, 2019.
64. A. Furfaro, P. Pace, and A. Parise, "Facing DDoS bandwidth flooding attacks," *Simulation Modelling Practice and Theory*, vol. 98, p. 101984, 2020.
65. R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 32, no. 3, pp. 62–73, 2002.
66. D. K. Y. Yau, J. C. S. Lui, F. Liang, and Y. Yam, "Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles," *IEEE/ACM Trans. Netw.*, vol. 13, no. 1, pp. 29–42, 2005
67. R. Chen and J.-M. Park, "Attack Diagnosis: Throttling distributed denial-of-service attacks close to the attack sources," in Proceedings. 14th International Conference on Computer Communications and Networks, ICCCN 2005, 2005, pp. 275–280.
68. K. Argyraki and D. R. Cheriton, "Scalable network-layer defense against internetbandwidth-floodingattacks,"*IEEE/ACMTrans.Netw.*,vol.17,no.4, pp. 1284–1297, 2009.
69. R. Xu, Y. Chen, E. Blasch, and G. Chen, "Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness," *Optical Engineering*, vol. 58, no. 4, p. 041609.
70. T. Llansó, M. McNeil, and C. Noteboom, "Multi-Criteria Selection of Capability-Based Cybersecurity Solutions," in Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019, January.

71. W. Wang, Q. Chen, X. He, and L. Tang, "Cooperative anomaly detection with transfer learning-based hidden markov model in virtualized network slicing," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1534–1537, 2019.
72. X. Liu, X. Yang, and Y. Lu, "To filter or to authorize: Network-layer DoS defense against multimillion-node botnets," in Proceedings of the ACM SIGCOMM 2008 conference on Data communication, 2008, pp. 195–206.
73. X. L. A. L. X. Yang and D. Wetherall, "Passport: Secure and adoptable source authentication."
74. J. Mirkovic, P. Reiher, and M. Robinson, "Forming alliance for DDoS defense," in New Security Paradigms Workshop, 2003, pp. 18–21.
75. M. S. Kang, V. D. Gligor, V. Sekar, et al., "SPIFFY: Inducing cost-detectability tradeoffs for persistent link-flooding attacks," in NDSS, 2016.
1. Anderson, R. "Why information security is hard—An economic perspective." In *Proceedings of the 17th Annual Computer Security Applications Conference*. New Orleans, LA, 2001.
2. Moore, David, and Shannon, Colleen. "Code-Red: A case study on the spread and victims of an Internet worm." Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement. ACM, 2002.
3. Nagurney, A., Yu, M., Masoumi, A. H., & Nagurney, L. S. (2013). *Networks against time: Supply chain analytics for perishable products*. Springer Science & Business Media.
4. Bohme, R., & Moore, T. (2010). The iterated weakest link. *IEEE Security & Privacy*, *8*(1), 53–55.
5. Laszka, A., Johnson, B., & Grossklags, J. (2018). On the assessment of systematic risk in networked systems. *ACM Transactions on Internet Technology (TOIT)*, *18*(4), 1–28.
6. Varian, H. (2004). System reliability and free riding. In *Economics of information security* (pp. 1–15). Springer, Boston, MA.
7. Feri, L., Nijssen, S. J. J., Baggen, C. P. M. J., Gritti, T., Rajagopalan, R., De Bruijn, F. J., & Yang, H. (2016). U.S. Patent No. 9, 386, 643. Washington, DC: U.S. Patent and Trademark Office.
8. Rosoff, H., Cui, J., & John, R. S. (2013). Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions*, *33*(4), 517–529.
9. Caputo, F., Scuotto, V., Carayannis, E., & Cillo, V. (2018). Intertwining the internet of things and consumers' behaviour science: Future promises for businesses. *Technological Forecasting and Social Change*, *136*, 277–284.
10. Li, Q., Meng, S., Zhang, S., Hou, J., & Qi, L. (2019). Complex attack linkage decision-making in edge computing networks. *IEEE Access*, *7*, 12058–12072.
11. Uslu, B., Eren, T., Gür, Ş., & Özcan, E. (2019). Evaluation of the difficulties in the internet of things (IoT) with multi-criteria decision-making. *Processes*, *7*(3), 164.

12. Novak, T. P., & Hoffman, D. L. (2019). Relationship journeys in the internet of things: A new framework for understanding interactions between consumers and smart objects. *Journal of the Academy of Marketing Science*, *47*(2), 216–237.
13. Nussbaum, B., & Sebastian Udoh, E. (2020). Surveillance, surveillance studies, and cyber criminality. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 155–182.
14. Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, *12*(5), 741–760.
15. Li, Y., Yazdanmehr, A., Wang, J., & Rao, H. R. (2019). Responding to identity theft: A victimization perspective. *Decision Support Systems*, *121*, 13–24.
16. Akinwumi, D. A., Iwasokun, G. B., Alese, B. K., & Oluwadare, S. A. (2017). A review of game theory approach to cyber security risk management. *Nigerian Journal of Technology*, *36*(4), 1271–1285.
17. Hyder, B., & Govindarasu, M. "Optimization of cybersecurity investment strategies in the smart grid using game-theory." In 2020 *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1–5). IEEE, 2020, February.
18. Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers*, *21*(5), 997–1018.
19. Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R., & Huth, M. (2018). Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance.
20. Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Rethinking information sharing for actionable threat intelligence. *arXiv preprint arXiv*,*1702*.00548.
21. Saenger, J., Mazurczyk, W., Keller, J., & Caviglione, L. (2020). VoIP network covert channels to enhance privacy and information sharing. *Future Generation Computer Systems*, 111, 96–106.
22. Guan, P., He, M., Zhuang, J., & Hora, S. C. (2017). Modeling a multitarget attacker–defender game with budget constraints. *Decision Analysis*, *14*(2), 87–107.
23. Cheung, K. F., & Bell, M. G. (2019). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. *European Journal of Operational Research*, 2019.
24. Cui, P., & Guin, U. "Countering botnet of things using blockchain-based authenticity framework." In 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) (pp. 598–603). IEEE, 2019, July.

25. Pijpker, J., & Vranken, H. "The role of Internet service providers in botnet mitigation." In 2016 European Intelligence and Security Informatics Conference (EISIC) (pp. 24–31). IEEE, 2016, August.
26. Hadlington, L. J. (2018). Employees' attitudes towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, *12*(1), 262–274.
27. Shankar, N., & Mohammed, Z. (2020). Surviving data breaches: A multiple case study analysis. *Journal of Comparative International Management*, *23*(1), 35.
28. Bhattacharya, P., & Guo, M. (2020). An incentive compatible mechanism for replica placement in peer-assisted content distribution. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, *12*(1), 47–67.
29. Ma, B. J., Zhou, Z. L., & Hu, F. Y. (2017). Pricing mechanisms in the online peer-to-peer lending market. *Electronic Commerce Research and Applications*, *26*, 119–130.
30. Cocchi, R., Shenker, S., Estrin, D., & Zhang, L. (1993). Pricing in computer networks: Motivation, formulation, and example. *IEEE/ACM Transactions on Networking*, *1*(6), 614–627.
31. MacKie-Mason, J. K., & Varian, H. R. (1995). Pricing the internet. *Public Access to the Internet*, *269*, 273.
32. Shenker, S., Clark, D., Estrin, D., & Herzog, S. (1996). Pricing in computer networks: Reshaping the research agenda. *ACM SIGCOMM Computer Communication Review*, *26*(2), 19–43.
33. Hayel, Y., Ros, D., & Tuffin, B. "Less-than-best-effort services: Pricing and scheduling." In IEEE *INFOCOM 2004* (Vol. 1). IEEE, 2004, March.
34. Kelly, F. P. (1997). Charging and accounting for bursty connections. *Internet Economics*, 253–278.
35. Keon, N., & Anandalingam, G. A. (2005). A new pricing model for competitive telecommunications services using congestion discounts. *INFORMS Journal on Computing, 17*(2), 248–262.
36. Clark, D. "Combining Sender and Receiver Payments in the Internet," http://www.gta.ufrj.br/DiffServ/csrp-ddc.ps.gz
37. Cocchi, R., Estrin, D., Shenker, S., & Zhang, L. (1991). A study of priority pricing in multiple service class networks. *ACM SIGCOMM Computer Communication Review*, *21*(4), 123–130.
38. Gupta, A., Stahl, D. O., & Whinston, A. B. (1997). Priority pricing of integrated services networks. *Internet Economics*, 323–352.
39. Odlyzko, A. "Paris metro pricing for the internet." In Proceedings of the 1st ACM conference on Electronic commerce (pp. 140–147), 1999, November.
40. Dube, P., Borkar, V. S., & Manjunath, D. "Differential join prices for parallel queues: Social optimality, dynamic pricing algorithms and application to internet pricing." In *Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies* (Vol. 1, pp. 276–283). IEEE, 2002, June.

41. Hande, P., Chiang, M., Calderbank, R., & Zhang, J. "Pricing under constraints in access networks: Revenue maximization and congestion management." In 2010 Proceedings IEEE INFOCOM (pp. 1–9). IEEE, 2010, March.
42. Nevo, A., Turner, J. L., & Williams, J. W. (2016). Usage-based pricing and demand for residential broadband. *Econometrica*, *84*(2), 411–443.
43. Kelly, F. P., Maulloo, A. K., & Tan, D. K. (1998). Rate control for communication networks: shadow prices, proportional fairness and stability. *Journal of the Operational Research society*, *49*(3), 237–252.
44. Keon, N., & Anandalingam, G. A. (2005). A new pricing model for competitive telecommunications services using congestion discounts. *INFORMS Journal on Computing*, *17*(2), 248–262.
45. Fankhauser, G., Stiller, B., Vögtli, C., & Plattner, B. "Reservation-based charging in an integrated services network." In 4th INFORMS Telecommunications Conference, Boca Raton, Florida, USA (Vol. 302, pp. 305–309), 1998, March.
46. Fankhauser, G., & Plattner, B. (1999, December). Diffserv bandwidth brokers as mini-markets. In Workshop on Internet Service Quality Economics, MIT, US.
47. Wang, X., & Schulzrinne, H. (2006). Pricing network resources for adaptive applications. *IEEE/ACM Transactions on Networking*, *14*(3), 506–519.
48. Semret, N., Liao, R. F., Campbell, A. T., & Lazar, A. A. (2000). Pricing, provisioning and peering: dynamic markets for differentiated Internet services and implications for network interconnections. *IEEE Journal on Selected Areas in Communications*, *18*(12), 2499–2513.
49. Wang, X., & Schulzrinne, H. (1999). A Framework for Resource Negotiation and Pricing in the Internet. Technical Report, Columbia University.
50. O'Donnell, A. J., & Sethu, H. (2003). Congestion control, differentiated services, and efficient capacity management through a novel pricing strategy. *Computer Communications*, *26*(13), 1457–1469.
51. Zhang, M., Gao, L., Huang, J., & Honig, M. L. (2019). Hybrid pricing for mobile collaborative Internet access. *IEEE/ACM Transactions on Networking*, *27*(3), 986–999.
52. Nguyen, T. T., & Armitage, G. J. (2005). Evaluating Internet Pricing Schemes: A Three-Dimensional Visual Model. *ETRI Journal*, *27*(1), 64–74.
1. Gonzalez, J. D. T., & Kinsner, W. (2016). Zero-crossing analysis of lévy walks and a DDoS dataset for real-time feature extraction: Composite and applied signal analysis for strengthening the internet-of-things against DDoS attacks. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, *8*(4), 1–28.
2. Bhushan, K., & Gupta, B. B. (2017). Security challenges in cloud computing: state-of-art. *International Journal of Big Data Intelligence*, *4*(2), 81–107.

3. Gou, Z., Yamaguchi, S., & Gupta, B. B. (2017). Analysis of various security issues and challenges in cloud computing environment: A survey. In Identity Theft: Breakthroughs in Research and Practice (pp. 221–247). IGI Global.
4. Kumar, A. (2019). Design of secure image fusion technique using cloud for privacy-preserving and copyright protection. *International Journal of Cloud Applications and Computing (IJCAC)*, *9*(3), 22–36.
5. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, *107*, 30–48.
6. Gupta, B. B. (2019). An efficient KP design framework of attribute-based searchable encryption for user level revocation in cloud. Concurrency and Computation: Practice and Experience, e5291.
7. Priyadarshinee, P. (2018). Cloud computing adoption: scale development, measurement and validation. *International Journal of Cloud Applications and Computing (IJCAC), 8*(1), 97–116.
8. Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. *IEEE Access*, *7*, 80813–80828.
9. VivinSandar, S., & Shenai, S. (2012). Economic denial of sustainability (EDoS) in cloud services using HTTP and XML based DDoS attacks. *International Journal of Computer Applications*, *41*(20).
10. Bhushan, K., & Gupta, B. B. (2019). Network flow analysis for detection and mitigation of Fraudulent Resource Consumption (FRC) attacks in multimedia cloud computing. *Multimedia Tools and Applications*, *78*(4), 4267–4298.
11. Monge, M. A. S., Vidal, J. M., & Pérez, G. M. (2019). Detection of economic denial of sustainability (EDoS) threats in self-organizing networks. *Computer Communications*, *145*, 284–308.
12. Aouzal, K., Hafiddi, H., & Dahchour, M. (2019). Policy-Driven Middleware for Multi-Tenant SaaS Services Configuration. *International Journal of Cloud Applications and Computing (IJCAC)*, *9*(4), 86–106.
13. Siva, T., & Krishna, E. P. (2013). Controlling various network based ADoS attacks in cloud computing environment: by using port hopping technique. *Int. J. Eng. Trends Technol*, *4*(5), 2099–2104.
14. Herzfeldt, A., Floerecke, S., Ertl, C., & Krcmar, H. (2019). Examining the antecedents of cloud service profitability. *International Journal of Cloud Applications and Computing (IJCAC)*, *9*(4), 37–65.
15. Al-Nawasrah, A., Almomani, A. A., Atawneh, S., & Alauthman, M. (2020). A survey of fast flux botnet detection with fast flux cloud computing. *International Journal of Cloud Applications and Computing (IJCAC)*, *10*(3), 17–53.
16. Jadad, H. A., Touzene, A., & Day, K. (2020). Offloading as a service middleware for mobile cloud apps. *International Journal of Cloud Applications and Computing (IJCAC)*, *10*(2), 36–55.

17. Velliangiri, S., Karthikeyan, P., & Vinoth Kumar, V. (2020). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *Journal of Experimental & Theoretical Artificial Intelligence*, 1–20.
18. Aldribi, A., Traoré, I., Moa, B., & Nwamuo, O. (2020). Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. *Computers & Security*, *88*, 101646.
19. Morbitzer, M., Huber, M., & Horsch, J. (2019, March). Extracting secrets from encrypted virtual machines. In Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (pp. 221–230).
20. Masood, M., Anwar, Z., Raza, S. A., & Hur, M. A. (2013, December). EDoS armor: A cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments. In INMIC (pp. 37–42). IEEE.
21. Baig, Z. A., Sait, S., & Binbeshr, F. S. (2016). U.S. Patent Application No. 14/970,152.
22. Saini, B., & Somani, G. (2014, March). Index page based EDoS attacks in infrastructure cloud. In International Conference on Security in Computer Networks and Distributed Systems (pp. 382–395). Springer, Berlin, Heidelberg.
23. Alosaimi, W., & Al-Begain, K. (2013, June). A new method to mitigate the impacts of the economical denial of sustainability attacks against the cloud. In Proceedings of the 14th Annual Post Graduates Symposium on the convergence of Telecommunication, Networking and Broadcasting (PGNet) (pp. 116–121).
24. Saravanan, A., Bama, S. S., Kadry, S., & Ramasamy, L. K. (2019). A new framework to alleviate DDoS vulnerabilities in cloud computing. *International Journal of Electrical & Computer Engineering*, 9(2088–8708).
25. Gumaei, A., Sammouda, R., Al-Salman, A. M. S., & Alsanad, A. (2019). Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation. *Journal of Parallel and Distributed Computing*, *124*, 27–40.
26. Jeyanthi, N., & Mogankumar, P. C. (2014). A virtual firewall mechanism using army nodes to protect cloud infrastructure from DDoS attacks. *Cybernetics and Information Technologies*, *14*(3), 71–85.
27. Jia, Q., Wang, H., Fleck, D., Li, F., Stavrou, A., & Powell, W. (2014, June). Catch me if you can: A cloud-enabled DDoS defense. In *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (pp. 264–275). IEEE.
28. Amazon Web Services, AWS best practices for DDoS resiliency, 2015, (https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf).

29. Rawashdeh, A., Alkasassbeh, M., & Al-Hawawreh, M. (2018). An anomaly-based approach for DDoS attack detection in cloud environment. *International Journal of Computer Applications in Technology*, *57*(4), 312–324.
30. Ghosh, P., Shakti, S., & Phadikar, S. (2016). A cloud intrusion detection system using novel PRFCM clustering and KNN based dempster-shafer rule. *International Journal of Cloud Applications and Computing (IJCAC)*, *6*(4), 18–35.
31. Shidaganti, G. I., Inamdar, A. S., Rai, S. V., & Rajeev, A. M. (2020). SCEF: A model for prevention of DDoS attacks from the cloud. *International Journal of Cloud Applications and Computing (IJCAC)*, *10*(3), 67–80.
32. Khan, M. S., Ferens, K., & Kinsner, W. (2015). Multifractal singularity spectrum for cognitive cyber defence in internet time series. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, *7*(3), 17–45.
33. Hammi, B., Rahal, M. C., & Khatoun, R. (2016, July). Clustering methods comparison: Application to source based detection of botclouds. In 2016 International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC) (pp. 1–7). IEEE.
34. Hammi, B., Zeadally, S., & Khatoun, R. (2019). An empirical investigation of botnet as a service for cyberattacks. *Transactions on Emerging Telecommunications Technologies*, *30*(3), e3537.
35. Rani, D. R., & Geethakumari, G. (2020). A framework for the identification of suspicious packets to detect anti-forensic attacks in the cloud environment. *Peer-to-Peer Networking and Applications*, 1–14.
36. Law, T. K., Lui, J., & Yau, D. K. (2005). You can run, but you can't hide: an effective statistical methodology to trace back DDoS attackers, parallel and distributed systems, *IEEE Transactions on Parallel and Distributed Systems*, *16*(9), 799–813.
37. Yu, S., Tian, Y., Guo, S., & Wu, D. O. (2013). Can we beat DDoS attacks in clouds? *IEEE Transactions on Parallel and Distributed Systems*, *25*(9), 2245–2254.
38. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). Service resizing for quick DDoS mitigation in cloud computing environment. *Annals of Telecommunications*, *72*(5), 237–252.
39. Gilad, Y., Herzberg, A., Sudkovitch, M., & Goberman, M. (2016). CDN-on-demand: An affordable DDoS defense via untrusted clouds. In NDSS.
40. Baciu, G., Wang, Y., & Li, C. (2017). Cognitive visual analytics of multidimensional cloud system monitoring data. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, *9*(1), 20–34.
41. Bhushan, K., & Gupta, B. B. (2019). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, *10*(5), 1985–1997.

42. Khor, S. H., & Nakao, A. (2011, July). DaaS: DDoS mitigation-as-a-service. In 2011 IEEE/IPSJ International Symposium on Applications and the Internet (pp. 160–171). IEEE.
43. Mathur, M., Madan, M., & Chaudhary, K. (2016). A satiated method for cloud traffic classification in software defined network environment. *International Journal of Cloud Applications and Computing (IJCAC)*, *6*(2), 64–79.
44. Nasiri, A. A., & Derakhshan, F. (2018). Assignment of virtual networks to substrate network for software defined networks. *International Journal of Cloud Applications and Computing (IJCAC)*, *8*(4), 29–48.
45. Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in internet-of-things (IoTs) framework. *Future Generation Computer Systems*, *108*, 909–920.
46. Gupta, B. B., & Agrawal, D. P. (Eds.). (2019). *Handbook of research on cloud computing and big data applications in IoT*. IGI Global.
47. Salim, M. M., Rathore, S., & Park, J. H. (2019). Distributed denial of service attacks and its defenses in IoT: A survey. *The Journal of Supercomputing*, 1–44.
48. Tewari, A., & Gupta, B. B. (2017). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing*, *73*(3), 1085–1102.
49. Zhang, Y., Li, P., & Wang, X. (2019). Intrusion detection for IoT based on improved genetic algorithm and deep belief network. *IEEE Access*, *7*, 31711–31722.
50. Tewari, A., & Gupta, B. B. (2019). A novel ECC-based lightweight authentication protocol for internet of things devices. *International Journal of High Performance Computing and Networking*, *15*(1–2), 106–120.
51. Deshmukh-Bhosale, S., & Sonavane, S. S. (2019). A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things. *Procedia Manufacturing*, *32*, 840–847.
52. Rajagopalan, A., Jagga, M., Kumari, A., & Ali, S. T. (2017, February). A DDoS prevention scheme for session resumption SEA architecture in healthcare IoT. In 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 1–5). IEEE.
53. Dao, N. N., Phan, T. V., Kim, J., Bauschert, T., & Cho, S. (2017). Securing heterogeneous IoT with intelligent DDoS attack behavior learning. *arXiv preprint arXiv,* 1711.06041.
54. Mehmood, A., Mukherjee, M., Ahmed, S. H., Song, H., & Malik, K. M. (2018). NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. *The Journal of Supercomputing*, *74*(10), 5156–5170.
55. Dao, N. N., Vu, D. N., Lee, Y., Park, M., & Cho, S. (2018, January). MAEC-X: DDoS prevention leveraging multi-access edge computing. In 2018 International Conference on Information Networking (ICOIN) (pp. 245–248). IEEE.

56. Bhardwaj, K., Miranda, J. C., & Gavrilovska, A. (2018). Towards IoT-DDoS prevention using edge computing. In {USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 18).
57. Sahi, A., Lai, D., Li, Y., & Diykh, M. (2017). An efficient DDoS TCP flood attack detection and prevention system in a cloud environment. *IEEE Access*, *5*, 6036–6048.
58. Doshi, R., Apthorpe, N., & Feamster, N. (2018, May). Machine learning ddos detection for consumer internet of things devices. In 2018 IEEE Security and Privacy Workshops (SPW) (pp. 29–35). IEEE.
59. Kawamura, T., Fukushi, M., Hirano, Y., Fujita, Y., & Hamamoto, Y. (2017, June). An NTP-based detection module for DDoS attacks on IoT. In *2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)* (pp. 15–16). IEEE.
60. McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018, July). Botnet detection in the internet of things using deep learning approaches. In 2018 international joint conference on neural networks (IJCNN) (pp. 1–8). IEEE.
61. Mondal, H. S., Hasan, M. T., Hossain, M. B., Rahaman, M. E., & Hasan, R. (2017, December). Enhancing secure cloud computing environment by Detecting DDoS attack using fuzzy logic. In 2017 3rd International Conference on Electrical Information and Communication Technology (EICT) (pp. 1–4). IEEE.
62. Yuan, X., Li, C., & Li, X. (2017, May). DeepDefense: Identifying DDoS attack via deep learning. In 2017 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 1–8). IEEE.
63. da Silva Cardoso, A. M., Lopes, R. F., Teles, A. S., & Magalhães, F. B. V. (2018, April). Real-time DDoS detection based on complex event processing for IoT. In 2018 *IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)* (pp. 273–274). IEEE.
64. Anirudh, M., Thileeban, S. A., & Nallathambi, D. J. (2017, January). Use of honeypots for mitigating DoS attacks targeted on IoT networks. In 2017 International conference on computer, communication and signal processing (ICCCSP) (pp. 1–4). IEEE.
65. Yin, D., Zhang, L., & Yang, K. (2018). A DDoS attack detection and mitigation with software-defined Internet of Things framework. *IEEE Access*, *6*, 24694–24705.
66. Bhunia, S. S., & Gurusamy, M. (2017, November). Dynamic attack detection and mitigation in IoT using SDN. In 2017 27th International telecommunication networks and applications conference (ITNAC) (pp. 1–6). IEEE.
67. Özçelik, M., Chalabianloo, N., & Gür, G. (2017, August). Software-defined edge defense against IoT-based DDoS. In 2017 IEEE International Conference on Computer and Information Technology (CIT) (pp. 308–313). IEEE.

68. Alharbi, T., Aljuhani, A., & Liu, H. (2017, January). Holistic DDoS mitigation using NFV. In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1–4). IEEE.
69. Liu Y., Dong M., Ota K., Li J., Wu, J. (2018). Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks. In 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, pp. 1–6.
1. Bhushan, K., & Gupta, B. B. (2019). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, *10*(5), 1985–1997.
2. Open Networking Foundation. (2020, September). [Online]. Available: https://www.opennetworking.org/
3. Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., & Rao, N. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. *IEEE Communications Magazine*, *51*(7), 36–43.
4. Jarraya, Y., Madi, T., & Debbabi, M. (2014). A survey and a layered taxonomy of software-defined networking. *IEEE Communications Surveys & Tutorials*, *16*(4), 1955–1980.
5. Nasiri, A. A., & Derakhshan, F. (2018). Assignment of virtual networks to substrate network for software defined networks. *International Journal of Cloud Applications and Computing (IJCAC)*, *8*(4), 29–48.
6. Mathur, M., Madan, M., & Chaudhary, K. (2016). A Satiated Method for Cloud Traffic Classification in Software Defined Network Environment. *International Journal of Cloud Applications and Computing (IJCAC)*, *6*(2), 64–79.
7. Singh, M. P., & Bhandari, A. (2020). New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges. Computer Communications, 154, 509–527.
8. Dahiya, A., & Gupta, B. B. (2019). A PBNM and economic incentive-based defensive mechanism against DDoS attacks. Enterprise Information Systems, 1–21.
9. Izumi, S., Hata, M., Takahira, H., Soylu, M., Edo, A., Abe, T., & Suganuma, T. (2017). A proposal of SDN based disaster-aware smart routing for highly-available information storage systems and its evaluation. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, *9*(1), 69–83.
10. Mishra, A., Gupta, N., & Gupta, B. B. (2020). Security threats and recent countermeasures in cloud computing. In *Modern Principles, Practices, and Algorithms for Cloud Security* (pp. 145–161). IGI Global.
11. Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, *12*(2), 493–501.

12. Kreutz, D., Ramos, F. M., & Verissimo, P. (2013, August). Towards secure and dependable software-defined networks. In *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined networking* (pp. 55–60).
13. P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, & G. Gu. (2012). A security enforcement kernel for openflow networks. In *Proceedings of First Workshop on Hot Topics in Software Defined Networks* (pp. 121–126).
14. Myint Oo, M., Kamolphiwong, S., Kamolphiwong, T., & Vasupongayya, S. (2019). Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN). *Journal of Computer Networks and Communications*.
15. Mousavi, S. M. (2014). *Early detection of DDoS attacks in software defined networks controller* (Doctoral dissertation, Carleton University).
16. Liyanage, M., Ylianttila, M., & Gurtov, A. (2014, June). Securing the control channel of software-defined mobile networks. In *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014* (pp. 1–6). IEEE.
17. Shin, S., Yegneswaran, V., Porras, P., & Gu, G. (2013, November). Avant-guard: Scalable and vigilant switch flow management in software-defined networks. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security* (pp. 413–424).
18. Klöti, R., Kotronis, V., & Smith, P. (2013, October). OpenFlow: A security analysis. In *2013 21st IEEE International Conference on Network Protocols (ICNP)* (pp. 1–6). IEEE.
19. Hamid, S., Bawany, N. Z., & Shamsi, J. A. (2017). ReCSDN: Resilient controller for software defined networks. *International Journal of Advanced Computer Science and Applications, 8*(8), 202–208.
20. Wang, Y., Hu, T., Tang, G., Xie, J., & Lu, J. (2019). SGS: Safe-guard scheme for protecting control plane against DDoS attacks in software-defined networking. *IEEE Access*, *7*, 34699–34710.
21. Koponen, T., Casado, M., Gude, N., Stribling J., Poutievski L., Zhu M., Ramanathan R., Iwata Y., Inoue H., Hama T., et al. (2010). Onix: A distributed control platform for large-scale production networks. *OSDI*, *10*, 1–6.
22. Hassas Yeganeh, S., Ganjali Y. (2012). Kandoo: A framework for efficient and scalable offloading of control applications. In *Proceedings of the First Workshop on Hot Topics in Software Defined Networks, HotSDN '12, Association for Computing Machinery*, New York, NY, USA (pp. 19–24).
23. Yu, M., Rexford, J., Freedman M. J., Wang, J. (2010). Scalable flow-based networking with DIFANE. In *Proceedings of the ACM SIGCOMM 2010 Conference, SIGCOMM '10, Association for Computing Machinery*, New York, NY, USA (pp. 351–362).

24. Erickson. D. (2013). The beacon openflow controller. In *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, HotSDN '13, Association for Computing Machinery*, New York, NY, USA (pp. 13–18).
25. Tootoonchian, A., Gorbunov, S., Ganjali, Y., Casado, M., Sherwood, R. (2012). On controller performance in software-defined networks. In 2nd USENIX Workshop on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services, Hot-ICE 12, USENIX Association, San Jose, CA.
26. DDoS threat report 2018 Q2, 2018, https://www.nexusguard.com/threatreport-q2-2018
27. Botelho, F., Bessani, A., Ramos, F. M., & Ferreira, P. (2014, September). On the design of practical fault-tolerant SDN controllers. In 2014 third European workshop on software defined networks (pp. 73–78). IEEE.
28. POX controller, https://openflow.stanford.edu/display/ONL/POX+Wiki.html, accessed: July 2020
29. Gude, N., Koponen, T., Pettit, J., Pfaff, B., Casado, M., McKeown, N., & Shenker, S. (2008). NOX: Towards an operating system for networks. *ACM SIGCOMM Computer Communication Review*, *38*(3), 105–110.
30. An instant virtual network on your laptop (or other PC), http://mininet.org/, (Accessed July 2020)
31. Wang, S. Y., Chou, C. L., & Yang, C. M. (2013). EstiNet openflow network simulator and emulator. *IEEE Communications Magazine*, *51*(9), 110–117.
32. Bhandari, A., Sangal, A. L., & Kumar, K. (2016). Characterizing flash events and distributed denial-of-service attacks: An empirical investigation. *Security and Communication Networks*, *9*(13), 2222–2239.
33. CAIDA Ddos attack dataset, 2007, https://www.caida.org/data/passive/ddos20070804_dataset.xml, July 2020
34. Oct 2016 DYN/DDoS attack, 2016, http://www.red5security.com/, (Accessed 23 July 2020)
35. Faghani, M. R., & Nguyen, U. T. (2019). Mobile botnets meet social networks: Design and analysis of a new type of botnet. *International Journal of Information Security*, *18*(4), 423–449.
36. Koshy, P., Koshy, D., & McDaniel, P. (2014, March). An analysis of anonymity in bitcoin using p2p network traffic. *In* International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg (pp. 469–485).
37. Peters, G. W. & Panayi, E. (2015). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money, *Social Science Research Network*.
38. Atzei, N., Bartoletti, M., & Cimoli, T. (2017, April). A survey of attacks on ethereum smart contracts (sok). In International *C*onference on *P*rinciples of *S*ecurity and *T*rust, Springer, Berlin, Heidelberg (pp. 164–186).

39. Vasek, M., Thornton, M., & Moore, T. (2014, March). Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In International conference on financial cryptography and data security, Springer, Berlin, Heidelberg (pp. 57–71).
40. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of blockchain technology: Pros, cons and SWOT. *Cluster Computing*, *22*(6), 14743–14757.
41. Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016, April). The blockchain as a software connector. In *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)* (pp. 182–191). IEEE.
42. Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. *Computer Communications*, *136*, 10–29.
43. Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, *126*, 45–58.
44. Gueta, G. G., Abraham, I., Grossman, S., Malkhi, D., Pinkas, B., Reiter, M., … & Tomescu, A. (2019, June). SBFT: A scalable and decentralized trust infrastructure. In *2019 49th Annual IEEE/IFIP international conference on dependable systems and networks (DSN)* (pp. 568–580). IEEE.
45. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017, October). A review on consensus algorithm of blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 2567–2572). IEEE.
46. Sharples, M. and Domingue, J. (2015). The blockchain and kudos: A distributed system for educational record, reputation and reward. In *Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015)*, Lyon, France (pp.490–496).
47. Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014, November). Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 15–29).
48. Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: a technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, *18*(3), 2084–2123.
49. Vukoli´c, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International Workshop on Open Problems in Network Security, Zurich, Switzerland (pp.112–125).
50. Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of the 2017 IEEE BigData Congress*, Honolulu, Hawaii, USA (pp.557–564).

51. Sompolinsky, Y., & Zohar, A. (2015, January). Secure high-rate transaction processing in bitcoin. In International Conference on Financial Cryptography and Data Security (pp. 507–527). Springer, Berlin, Heidelberg.
52. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 17–30).
53. Karame, G., Androulaki, E., & Capkun, S. (2012). Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin. *IACR Cryptol. ePrint Arch.*, 2012(248).
54. Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10), 1.
55. Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart city. *Journal of Information Processing Systems*, *13*(1), 184–195.
56. Leiding, B., Memarmoshrefi, P., & Hogrefe, D. (2016, September). Self-managed and blockchain-based vehicular ad-hoc networks. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* (pp. 137–140).
57. Travis W. What is the ARK SmartBridge, and How Does it Work? Available: https://blog.ark.io/what-is-the-ark-smartbridge-and-how-does-it-work-1dd7fb1e17a0
58. Ouaguid, A., Abghour, N., & Ouzzif, M. (2018). A novel security framework for managing android permissions using blockchain technology. *International Journal of Cloud Applications and Computing (IJCAC)*, *8*(1), 55–79.
59. Sumathi, M., & Sangeetha, S. (2020). Blockchain based sensitive attribute storage and access monitoring in banking system. *International Journal of Cloud Applications and Computing (IJCAC)*, *10*(2), 77–92.
60. Singh, N., & Vardhan, M. (2019). Distributed ledger technology based property transaction system with support for iot devices. *International Journal of Cloud Applications and Computing (IJCAC), 9*(2), 60–78.
61. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In *Proceedings of IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA (pp. 839–858).
62. Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*, *132*, 1815–1823.
63. Joshi, A. P., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing, 1*(2), 121.
64. Bahack, L. (2013). Theoretical bitcoin attacks with less than half of the computational power (draft). *arXiv preprint arXiv*, *1312.7013*.

65. Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C. A., Kwiat, K. A., & Njilla, L. (2017, May). Security implications of blockchain cloud with analysis of block withholding attack. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)* (pp. 458–467). IEEE.
66. Kim, S. K., Kim, U. M., & Huh, J. H. (2019). A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security. *Energies*, *12*(3), 402.
67. Rosenfeld, M. (2014). Analysis of hashrate-based double spending. *arXiv preprint arXiv*, *1402*.2009.
68. Singh, A. (2006). Eclipse attacks on overlay networks: Threats and defenses. In *IEEE INFOCOM*.
69. Courtois, N. T., & Bahack, L. (2014). On subversive miner strategies and block withholding attack in bitcoin digital currency. *arXiv preprint arXiv*, *1402*.1718.
70. Song, G., Kim, S., Hwang, H., & Lee, K. (2019, January). Blockchain-based notarization for social media. In *2019 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1–2). IEEE.