A Survey on Distributed Denial of Service (DDoS) Attacks on Cloud Computing

Syed Abed Hossain
Department of CSE
BRAC University
Dhaka, Bangladesh
syed.abed.hossain@g.bracu.ac.bd

Quazi Shahriar Haq
Department of CSE
BRAC University
Dhaka, Bangladesh
quazi.shahriar.haq@g.bracu.ac.bd

Ahnaf Hossain Siddique
Department of CSE
BRAC University
Dhaka, Bangladesh
ahnaf.hossain.siddique@g.bracu.ac.bd

Mobassira Atia
Department of CSE
BRAC University
Dhaka, Bangladesh
mobassira.atia@g.bracu.ac.bd

Dipta Roy
Department of CSE
BRAC University
Dhaka, Bangladesh
dipta.roy@g.bracu.ac.bd

Zahid Hasan
Department of CSE
BRAC University
Dhaka, Bangladesh
zahid.hasan2@g.bracu.ac.bd

MD. Mustakin Alam
Department of CSE
BRAC University
Dhaka, Bangladesh
md.mustakin.alam@g.bracu.ac.bd

Md Humaion Kabir Mehedi
Department of CSE
BRAC University
Dhaka, Bangladesh
humaion.kabir.mehedi@g.bracu.ac.bd

Annajiat Alim Rasel
Department of CSE
BRAC University
Dhaka, Bangladesh
annajiat@bracu.ac.bd

***Abstract*—Cloud Computing provides the services required for various business operations like maintaining storage, computing capability, hardware requirements, and much more over the Internet. Security issues related to cloud computing are relevant to various stakeholders for an informed cloud adoption decision. Apart from data breaches, the cyber security research community is revisiting the attack space for cloud-specific solutions as these issues affect the budget, resource management, and service quality. Denial-of-Service (DoS) attacks and Distributed-Denial-of-Service (DDoS) attacks can primarily compromise the availability of the system services. DDoS attacks in cloud computing environments are growing due to the essential characteristics of cloud computing. They can be quickly started using various tools, leading to financial damage or affecting reputation. These attacks are complicated to detect and filter since the packets that cause the attack are similar to legitimate traffic. DDoS attacks are considered the biggest threat to the IT industry, and the intensity, size, and frequency of the attack are observed to increase yearly. This paper provides a detailed discussion of the different security issues on cloud computing, especially the effects of DDoS attacks, existing defense mechanisms, and ways to prevent them. This survey paper aims to highlight the severity of DDoS attacks and summarize the immense efforts made every day throughout the world to prevent DDoS attacks.**

***Index Terms*—Cloud Computing, DDoS Attack, Cloud Security, Distribute Computing System, Network Layers**

I. Introduction to Cloud Computing and DDoS Attack

Cloud computing is gaining popularity in academia and business because of its key properties, which include on-demand self-service, broadband network connectivity, resource pooling, quick flexibility, and measurable service. It offers substantial advantages [1]–[3] over traditional computer paradigms, such as lower capital cost (CapEx) and operational expense (OpEx). Cloud computing would not be conceivable without the underpinning support of networking. Software as a Service (SaaS) allows users to run and utilize software/applications [4], [5] without having to install them on their machines. A cloud provider, in particular, is an Infrastructure as a Service (IaaS) provider, which offers virtual machines (VMs) on demand.

DDoS attacks are becoming more common as networks migrate to cloud computing settings. DDoS attacks increased by 200 percent [6], [7] in the fourth quarter of 2012, according to Akamai Technologies. Some basic mitigation strategies, such as synchronous cookies or restricting connection time and capacity, can be used.

In sections II, we have discussed various security issues in cloud computing. Then in sections III, have summarized various components of DDoS attacks. In section IV, a detailed

discussion about the classification of DDoS attacks has been placed. In section V, have summarized various techniques for defending against DDoS attacks and in section VI, have mentioned some of the popular ways of defeating DDoS attacks. Finally, with section VII, we conclude this paper with a conclusion.

II. Security Issues in Cloud Computing

DoS attacks pose a significant risk to the Cloud environment as well as any network, including IoT. As a result, securing the Cloud environment safeguards the website [8], [9], [10], [11] it hosts as well as any devices linked to Cloud servers.

Security needs are becoming increasingly important as cloud usage grows. Different levels of security are required for different Cloud service users. A Cloud service [12], [13], [14], [15] user might be a single individual, a group of software developers, an academic organization, or a major corporation. Each with its unique set of requirements.

[16], [17] According to the service supplied, there are three forms of Cloud computing, as stated in the previous section: SaaS, PaaS, and IaaS. Cloud companies must ensure client data security to earn their confidence. Insider breaches, application vulnerabilities, and system availability [18], [19] are all risks. PaaS provides the developer with an environment in which to construct an application. Hackers can use this PAAS capability [16], [20] to try to manipulate the infrastructure. The following are the security concerns that both the Cloud user and the Cloud supplier must address:

A. Data-related issues

Cloud providers must maintain the security of data submitted by Cloud users and prevent security breaches to the greatest extent practicable. Providers should utilize strong encryption techniques to ensure optimal data security, as well as a variety of authorization procedures to manage data access. Data kept in the cloud should be kept distinct from data kept by other users.

B. Data integrity

ACID qualities can be used to maintain data integrity in standalone systems (atomicity, consistency, isolation, durability). This may be accomplished in distributed systems by utilizing a centralized global transaction manager. However, with cloud computing, integrity is a major issue. Inadequate data integrity measures might cause serious difficulties. Leaving this to the API level is an option, but standards such as WS-transaction and WS-reliability are not yet developed.

C. PaaS-related issues

A PaaS provider allows users to create applications on top of the platform. The provider must ensure that no unauthorized data is sent across applications. Some measures, like vulnerability ratings and patch coverage, can reflect application code quality. Hackers will most likely target visible code or infrastructure and do intensive black box testing.

D. IaaS-related issue

In IaaS, virtualization can cause a slew of security issues. The security duties of both the supplier and the client vary greatly depending on the type of Cloud service model. To ensure optimum trust and security in a Cloud resource, many strategies must be used.

E. Securing hypervisor

The hypervisor's principal job is to allocate resources to each virtual machine that is linked to a user on the Cloud. Any flaw in the operation of these hypervisors might jeopardize the security of all the virtual machines running on that hardware.

F. Side-channel attacks

These attacks are carried out by an attacker who resides on the victim's virtual machines. The attacker uses the private information as a decryption key to read the victim's encrypted data.

III. Components of DDoS Attacks on Cloud Computing

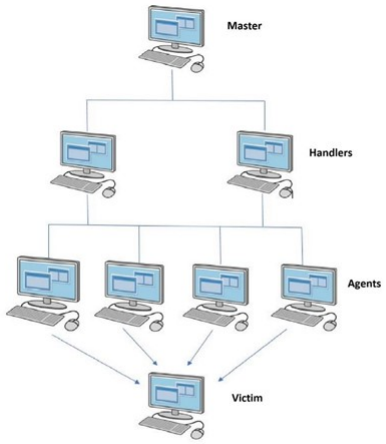

Fig. 1. Components of DDoS Attacks

The attacker begins by selecting either Agents or Botnets, also referred to as Zombies (described before). These Bots

then target a machine that is called the victim and are controlled remotely by the Bot-master as demonstrated in Figure 1. The attack spreads out and gets more disruptive with an increased number of zombies. The victim would be overloaded with heavy traffic, making it impossible for genuine users to access the services.

Cloud services offered to consumers will eventually stop working when the cloud server slowly reaches the "Service Denial" threshold. Due to the cloud service provider's (CSP) [7] overspending and subsequent on-demand resource invoicing, this results in a loss of money.

Various DDoS attacks are launched applying diverse protocols, including TCP, ICMP, and UDP. [21] In response to the attacker's flood of SYN [22], [23] requests, the victim recognizes the attack's SYN flooding and responds with SYNACK. However, the attacker never acknowledges the ACK, overloading the victim and ultimately resulting in a denial of service.

In the Ping of Death, the attacker sends the victim numerous packets [22] of malicious pings that, when modified at their destination, appear to be meaningless. The packets are eventually rejected, but the bandwidth had already been used, preventing the service from being accessed by genuine users. The LAND attack is initiated by sending more TCP packets [22] with the same source and destination IP addresses. The server goes down as a result of the victim continuously replying to itself.

[22], [23], [24] Using an ICMP packet, a different kind of Ping flood attack is conducted. Without waiting for a response, this kind of attack constantly sends a lot of echo requests. This gradually uses up the bandwidth and causes the server to crash.

The Smurf attack is carried out by sending an ICMP echo over the whole network using a fake IP address that corresponds to the target. As soon as a response to a request is received, the attack begins by focusing on the victim's ping response. This causes the victim flooding [25] and a denial of service as a result .

IV. Classification of DDoS Attack

DDoS attackers mostly target on following resources [26] and services:

- Computational resource consumptions (bandwidth, disk space, etc.)
- Disruption of configuration information (such as routing information)
- Disruption of state information, and disruption of physical network components.

There are many ways DDoS attacks are initiated and the attackers are inventing new ways day-by-day. In this section, we will try to classify types of DDoS attacks. The classification of DDoS attacks is mostly divided into three ways: application Layer attacks, protocol-based attacks, and volume-based attacks or volumetric attacks.

A. Application Layer attacks

Application layer or layer 7 attacks are also viewed as resource-based attacks. Attacks on this layer affect legitimate users by disrupting their access to web application services. Such attacks are difficult to detect [27], [28], [29] because most of the time, the attackers make legitimate requests like website users, and few bots are needed to attack.

1) Reflection/Amplification-based flooding attacks: A DNA amplification attack is used to use both reflection and amplification techniques. These attacks were used to send spoofed application layer protocol requests. With respect to DNS, response messages are always much larger than query messages. Therefore, attackers use spoofed source IP addresses to generate large amounts of network traffic. This generated flood of traffic is routed to the target system and partially or completely disabled.

2) HTTP flooding attacks: An attacker sends a legitimate HTTP request to the server. Her requests in the attack resemble regular HTTP requests. This request volume is so large that it consumes the target's resources and leads to denial of service. HTTP flooding attacks can be categorized into the following

- *Session flooding attacks:* In this type of attack, the attacker's connection request rate for sessions is higher than legitimate user requests. This consumes most of the server's resources and causes flood attacks. HTTP get/post flooding is an example of this category.
- *Request flooding attacks:* An attacker sends a session with more requests than usual, causing a DDoS flooding attack on the server. Single-session HTTP gets/post-flooding attacks (also known as excessive single-session VERB) are the most prominent attacks in this category. This is a variant of an earlier attack that uses HTTP 1.1 features to allow multiple requests within a single session.

3) Asymmetric attack: An attacker constructs a single packet that encapsulates multiple requests. In this way, even at low attack packet rates, the attacker can keep the victim's server under high load. This makes the attacker almost invisible. Some of the most common attacks in this category are listed below.

4) Slow Request/Response Attacks: Sessions that contain high-workload requests are sent by attackers to make the overall response from the server slower. Examples of attacks in this category include those presented by Shekyan (2012), Bhuvaneswari and Rauf (2009) and Poornaselvan et al. (2008). Slow post-attack: Attacker sends complete HTTP

header and keeps awaiting server to get further message body, also known as slow request bodies.

B. Protocol-based attack

Attackers launch this kind of attack using UDP, TCP, DNS, and ICMP protocol packets. The attacker floods the target with connections that consume the target's resources. This type of attack often works at layers 3 and 4 of the OSI model on network devices like routers. The protocol-based attack [29] can be categorized into four parts. They are,

1) Normal flooding attacks: Attackers attempt to exploit the victim's network bandwidth. Examples of normal flooding attacks include UDP floods, ICMP floods, DNS floods, and VoIP flood attacks. All of these can be carried out by spoofed or non-spoofed IP addresses.

2) Protocol exploitation flooding attacks: A protocol exploit flooding attack is a type of denial-of-service attack. Attackers focuses on implementation flaws in the victim's protocol. Examples of protocol exploit floods include TCP SYN floods, RST/FIN floods, and ACKandPUSH ACK floods.

3) Reflection-based flooding attacks: Reflector attacks are similar to Smurf and Fraggle attacks in nature. Attackers target reflectors by sending forged ICMP echo requests. Reflectors send replies according to the request, rather than direct requests to the victim as this eats up resources.

4) Amplification-based flooding attacks: Smurf attacks use a technique called reflection and amplification to increase traffic to the victim. Reflection and amplification techniques are always used with the help of botnets, or internet address-switching enabled by Microsoft Windows operating system.

C. Volume-based attacks

Volume-based attacks include UDP and ICMP flood attack. Bot-net-based DDoS attacks can be considered under this category. A detailed description of DDoS volumetric and protocol attacks has been discussed by Saman Taghavi Zargar, James Joshi, and David Tipper. It can be divided into IRC-based botnets [29] and Web-based botnets .

1) IRC-based Botnets: Hackers can easily hijack a chatbot to send commands to themselves and spread malicious code across the internet by abusing an IRC channel's address barreling through thousands of servers.

2) Web-based Botnets: Communicating over HTTP complicates the process all the way back to the command-and-control structure. Complex PHP scripts are used to configure and control web-based bots. Stealthier than IRC-based botnets, as they can hide in legitimate HTTP traffic.

Till now we have discussed the DDoS attack category based on their attacking behaviors on cloud computing. However, a DDoS attack can be classified also by the attacker's motivation. DDoS attack can be classified into five categories based on the attacker's motive.

- *Economic gain:* This kind of attack is often targeted at corporations. Most experienced and technical attackers become involved, as the incentive nature is very high [30], [31], [32], [22], [33] in this kind of motive-based attack.
- *Revenge:* Attackers of this category are mostly frustrated individuals, who usually carry out this kind of attack as a response to perceived injustice.
- *Ideological belief:* Attackers of this category are motivated by ideological beliefs. This is currently one of the reasons for increasing DDoS attacks. For example, political reasons have led to recent disruptions in Estonia in 2007, Iran in 2009, and WikiLeaks in 2010.
- *Intellectual challenges:* Attackers in this category are usually young hacking enthusiasts who initiate DDoS attacks as experiments. Also, to invent/evolve DDoS attacking methods this group of attackers practices DDoS attacks.
- *Cyber warfare:* Attackers in this category usually belong to a country's military or terrorist organization. They have political motives for broadly attacking important sectors of other countries.

The effects of these attacks can be direct or indirect. Direct effects can be loss of business and revenue, and indirect effects include additional energy consumption, component damage, mitigation costs, and reputational damage.

V. Defense mechanism against DDoS [34]

Various solutions have been proposed and applied by researchers to guard against DDoS attacks. These countermeasures generally consist of two steps: Detection and IP traceback.

A. Detection

The first and most crucial stage in defending against DDoS attacks is detection. Activity profiling, packet filtering, sequential change-point detection, wavelet analysis, and other techniques are used to detect DDoS attacks. Unfortunately, because of the Internet's open architecture, hackers can use IP spoofing to hide the source address of attack packets in order to avoid source address detection. Attackers can also manipulate the TTL value of attack packets by modifying the hop distance between bots and victims in order to avoid hop count detection. Along with these, attackers also imitate flash crowds, which are brief spikes in regular traffic, to mask their attacks.

1) Feature Based Detection Method: Anomaly detection is a popular technique for DDoS detection. Finding typical patterns in the research objects and eliminating them is

the process of anomaly detection. By its very nature, this technique inherits false negatives and false positives. A hop-count filter is a successful strategy to combat source IP spoofing. Hops taken by an IP packet reaching the destination cannot be forged but any IP header information can be. Also, hop count information can be deducted from the IP header's TTL field. Additionally, it is easier to create an IP-to-hop-count (IP2HC) mapping table that comprises the destination IP address and necessary hop counts. Defenders can distinguish between authentic IPs and faked IPs using this table. Three phases of analysis are done on the detection rate.

- Single source.
- multiple sources.
- multiple sources with an awareness of the detection method.

2) Network Traffic Based Detection: The Internet's network traffic is a crucial component, making it a potent tool for DDoS detection at the network layer. System administrators can control and set up routers in a local area network. As a result, the routers can work together to jointly identify potential attacks. All passing packets with the same destination address are grouped together as one flow at each router in a local area network.

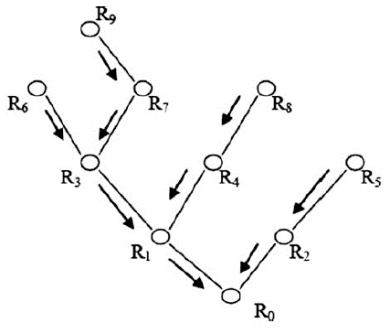

Fig. 2. A DDoS attack tree in a local area network [34]

In Figure 2, Router R0 is attached to the victim., whereas the local area network's edge is served by routers R6, R9, R8, and R5, respectively. Before moving on to any analysis, it is essential to understand what a flow is.

In the case of a continuing DDoS attack, there is just one flow that is directed at the victim. It is known as attack flow. There are numerous additional flows occurring at the same moment that are directed in various directions. Unlike the source address or TTL values, the victim's address is disclosed, making it impossible for hackers to fake or change the attack flow. As a result, flow-based detection can handle new kinds of flooding attacks and is not dependent on any particular attack features. Once the flows are established, metrics are required to gauge the flows in order to find anomalies.

An important metric in information theory is entropy. In the absence of a DDoS attack, a router's flow entropy stays within a narrow range. As soon as an attack occurs, the flow entropy plummets significantly because one or more flows are taking control of the routers.Therefore, the detection objective is to determine an appropriate threshold, Δ, for the reduction of flow entropy. A DDoS attack occurs when the flow entropy variation is equal to or higher than Δ.

3) Detection Against Mimicking Attacks: A Mimicked User Browsing DDoS attack involves botnets that pose as legitimate users attempting to access a server. Because Mimicked User Browsing is designed to replicate the activity of a legitimate human browsing, it is difficult to detect. The server will quickly become heavily loaded as the bots outnumber the actual users, making it difficult to service legitimate requests. A common method used to prevent this kind of DDoS attack is to use some kind of captcha controls, displaying images or patterns which a human is capable of responding to, but a bot would struggle with. Other DDoS mitigation methods for mimicked user browsing involve using behavioral analysis and advanced traffic analysis to analyze the user behavior and request patterns, attempting to learn the difference between legitimate user behavior and the bot attacks.

B. IP traceback [34]

Finding the attack sources, sometimes referred to as IP traceback is crucial for cyber security. IP traceback is currently defined as locating the gateways or routers that are most nearby to the actual sources of attack packets. An attack packet's source and attack path cannot be ascertained by the victim since the Internet has no memory and source IP spoofing is simple to do in attack packets. As a result, Internet router cooperation is required for all traceback systems. However, not all routers will necessarily take part in the traceback procedure. Since routers R2 and R4 are non-participating routers on the attack path R1 - R2 - R3 - R4 in Figure 3, it is possible to only go as far back as R3 even though R4 is the leaf node. The leaf node R8 may be traced even if some non-participating routers are present on the attack path for the alternate attack path R5 - R6 - R7 - R8.

The two groups of existing IP traceback techniques are network traffic-based techniques and packet marking techniques.

1) Probabilistic Packet Marking Based Traceback: The PPM method involves tagging packets arriving at participating domains, such as ISP networks, with special markings. The PPM technique can only identify the source nodes that are situated inside its domain, often far from the attacking

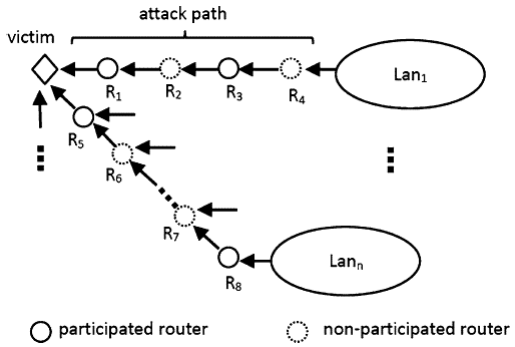

Fig. 3. Diagram of a DDoS attack in an online setting [34]

bots. PPM methods have a storage capacity issue when they store a lot of marked packets in order to reconstruct the attack tree. Due to the fact that attackers can send the victim forged marking information, the victim may be duped.

2) Deterministic Packet Marking Based Traceback: The DPM technique seeks to mark packets that came from nearby attack routers. Compared to PPM systems, the DPM methods lessen the demand on storage and power at the victim side. The biggest problem with current DPM systems is scalability. An IPv4 packet only has 25 free bits available, its difficult to cite every online source.

3) Network Traffic-Based Traceback Mechanism: The approach operates at the network layer and is flow-based. Once a DDoS attack has been detected, the victim determines which of its upstream routers are in the attack tree based on the flow entropy variations it has accumulated. Based on the observed local entropy fluctuations, the upstream routers may determine where the attack flows originated. High latency between the victim and attackers is the key factor influencing how long it takes to complete the traceback.

4) Marking on Demand Traceback Scheme: DDoS attacks often involve an increase in the number of packets sent to victims. Only when the increase in attack packets is considerable can DDoS attacks be detected. In order to solve the scalability problem of the DPM method, the marking on Demand (MOD) technique is created. The MOD system dynamically assigns DDoS attack-related marking IDs to routers to perform traceback operations.

VI. Ways of defeating DDoS attack

DDoS attacks are showing a practically yearly evolution as they spread throughout most businesses, from local schools to government agencies. Developing a defense against DDoS attacks is undoubtedly crucial. Attacks may be much harder to mitigate now than in the past because hackers and security generation are both becoming smarter. Because the attacks keep changing, businesses should be prepared with mitigating techniques.

DDoS mitigation comes in 3 models:

A. Scrubbing Centers

The most commonplace DDoS mitigation option for businesses is to look into gaining access to a cleaning center supplier. This can be used to thwart both volumetric and software-based attacks and is best suited for setups with several ISPs. A few organizations can absolutely be a tool for your data center to increase security, but this option isn't as cost-effective as the cloud-based one.

B. ISP- Clean Pipes Approach

Internet Service Providers (ISPs) are providing a range of services to their customers, including bandwidth, web hosting, and DDoS mitigation. Many ISPs have started their own internal scrubbing facilities [35] and, in exchange for a premium, will monitor and reduce attacks on the websites of their clients. Some ISPs are better than others at this, so customers should be sure to thoroughly examine and study the quality of the service offered by their ISPs.

C. Content Delivery Network Approach

Websites are kept globally on a few servers rather than one starting server because to the distributed nature of content transport networks (CDNs), which makes them difficult to shut down. Large CDNs can also contain over 100,000 servers that are used to distribute or cache internet content globally. However, since transferring content to a CDN can be a time-consuming undertaking, CDN-based comprehensive mitigation is only a reasonable choice for businesses that need core CDN capability.

Defeating an Attack this is Already Underway: In a few minutes, a suitable cloud security solution can be configured and running on the public cloud. An employer might request that all incoming visitors be routed through this platform [36], [37] for cleansing in response to requests made by skip-through users. Before the hostile traffic can get to the included community, it might be prevented. When necessary, bandwidth and other resources will scale automatically; only the capacity of the global cloud will be limited.

Therefore, we can say that the preventative plan for major organizations consists of the following 4 steps:

D. Organize a DDoS Attack Response Plan

Employers need to be prepared in the event of a DDoS attack. A response strategy should outline a way to maintain business operations, as well as what skills are required to deal with such an attack. Create an incident response team and define roles, along with contacting important stakeholders.

E. Secure your Infrastructure with DDoS Attack Prevention Solutions

Build multi-stage safety measures into your infrastructure, applications, and community. This may include firewalls, VPNs, anti-spam, content filtering, and other security measures. If you are looking for security by utilizing cloud-based comprehensive solutions, consider going "full cloud".

F. Perform a Network Vulnerability Assessment

Find the network's weak points before a hostile user does. This is done by making a list of all the devices in the network, together with their function, device information and any vulnerabilities associated with them.

G. Identify Warning Signs of a DDoS Attack

Early identification of a DDoS attack's warning indicators would allow you to move and, perhaps, reduce damage. Inform your team on the signs and symptoms of DDoS attacks so that everyone can be vigilant. Outsourcing DDoS assault prevention to the cloud has many benefits.

VII. Conclusion

DDoS attacks are rising every day in cloud computing. This paper tries to provide a detailed survey analysis on various aspects of DDoS attacks and sheds light on several techniques that are being used to defend against DDoS attacks every day. The goal of this survey paper is to showcase strategies and research done to mitigate DDoS attacks and to inspire security researchers to build effective DDoS detection and mitigation solutions in a cloud environment.

References

[1] Ying-Dar Lin, Dan Pitt, David Hausheer, Erica Johnson, and Yi-Bing Lin. Software-defined networking: Standardization for cloud computing's second wave. *Computer*, 47(11):19–21, 2014.

[2] Ray-I Chang and Chi-Cheng Chuang. A service-oriented cloud computing network management architecture for wireless sensor networks. *Ad-hoc & sensor wireless networks*, 22(1-2):65–90, 2014.

[3] Zhiyuan Yin, F Richard Yu, Shengrong Bu, and Zhu Han. Joint cloud and wireless networks operations in mobile cloud computing environments with telecom operator cloud. *IEEE Transactions on Wireless Communications*, 14(7):4020–4033, 2015.

[4] Mark Yep-Kui Chua, F Richard Yu, and Shengrong Bu. Dynamic operations of cloud radio access networks (c-ran) for mobile cloud computing systems. *IEEE Transactions on Vehicular Technology*, 65(3):1536–1548, 2015.

[5] Zhifeng Xiao and Yang Xiao. Security and privacy in cloud computing. *IEEE communications surveys & tutorials*, 15(2):843–859, 2012.

[6] Abdul Majid Farooqi, Tabrez Nafis, and Kafiyah Usvub. The notorious nine: Top cloud computing security challenges in 2017. *International Journal of Advanced Research in Computer Science*, 8:5, 07 2017.

[7] D Linthicum. As cloud use grows so will rate of ddos attacks. *InfoWorld. February 5th*, 2013.

[8] Esraa Alomari, Selvakumar Manickam, BB Gupta, Parminder Singh, and Mohammed Anbar. Design, deployment and use of http-based botnet (hbb) testbed. In *16th International Conference on Advanced Communication Technology*, pages 1265–1269. IEEE, 2014.

[9] Priyanka Negi, Anupama Mishra, and Brij B Gupta. Enhanced cbf packet filtering method to detect ddos attack in cloud computing environment. *arXiv preprint arXiv:1304.7073*, 2013.

[10] Meghna Chhabra, Brij Gupta, and Ammar Almomani. A novel solution to handle ddos attack in manet. 2013.

[11] PK Agrawal, Brij B Gupta, and Satbir Jain. Svm based scheme for predicting number of zombies in a ddos attack. In *2011 European Intelligence and Security Informatics Conference*, pages 178–182. IEEE, 2011.

[12] Michael Missbach, Thorsten Staerk, Cameron Gardiner, Joshua McCloud, Robert Madl, Mark Tempes, and George Anderson. Securing sap on the cloud. In *SAP on the Cloud*, pages 75–120. Springer, 2016.

[13] Massimo Ficco and Massimiliano Rak. Economic denial of sustainability mitigation in cloud computing. In *Organizational Innovation and Change*, pages 229–238. Springer, 2016.

[14] Subashini Subashini and Veeraruna Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1):1–11, 2011.

[15] Deyan Chen and Hong Zhao. Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering*, volume 1, pages 647–651. IEEE, 2012.

[16] Kai Hwang, Sameer Kulkareni, and Yue Hu. Cloud security with virtualized defense and reputation-based trust mangement. In *2009 Eighth IEEE international conference on dependable, autonomic and secure computing*, pages 717–722. IEEE, 2009.

[17] Omkar P Badve, Brij B Gupta, Shingo Yamaguchi, and Zhaolong Gou. Ddos detection and filtering technique in cloud environment using garch model. In *2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)*, pages 584–586. IEEE, 2015.

[18] Akhil Behl. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In *2011 World Congress on Information and Communication Technologies*, pages 217–222. IEEE, 2011.

[19] Juhi Sharma and Kshitiz Saxena. Cloud security challenges. *International Journal Computer Science and Information Technologies*, 3(3):4514–4515, 2012.

[20] Diogo AB Fernandes, Liliana FB Soares, João V Gomes, Mário M Freire, and Pedro RM Inácio. Security issues in cloud environments: a survey. *International Journal of Information Security*, 13(2):113–170, 2014.

[21] Abdul Moqeet. A machine learning based classification technique to detect ddos attack in cloud computing environment. *CAPITAL UNIVERSITY*, 2021.

[22] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, and Muttukrishnan Rajarajan. Ddos victim service containment to minimize the internal collateral damages in cloud computing. *Computers & Electrical Engineering*, 59:165–179, 2017.

[23] Mudit Rathore and Abhishek Vaish. A system design for multi-phase, hybrid ddos detection. *Computer Fraud & Security*, 2020(11):10–19, 2020.

[24] Basheer Al-Duwairi, Öznur Özkasap, Ahmet Uysal, Ceren Kocaoğullar, and Kaan Yildirim. Logdos: A novel logging-based ddos prevention mechanism in path identifier-based information centric networks. *Computers & Security*, 99:102071, 2020.

[25] Opeyemi Osanaiye, Kim-Kwang Raymond Choo, and Mqhele Dlodlo. Distributed denial of service (ddos) resilience in cloud: Review and conceptual cloud ddos mitigation framework. *Journal of Network and Computer Applications*, 67:147–165, 2016.

[26] Harshita Harshita. Detection and prevention of icmp flood ddos attack. *International Journal of New Technology and Research*, 3(3):263333, 2017.

[27] Shakti Arora and Arushi Bansal. Survey on prevention methods on ddos attacks. *International Journal of Advance Research in Computer Science and Software Engineering*, 4(7), 2014.

[28] Aanshi Bhardwaj, Veenu Mangat, Renu Vig, Subir Halder, and Mauro Conti. Distributed denial of service attacks in cloud: State-of-the-

art of scientific and commercial solutions. *Computer Science Review*, 39:100332, 2021.

[29] Kesavamoorthy Rajamannar, Alaguvathana Paravel, Suganya Rangasamy, and Vigneshwaran Pandi. Classifications of ddos attack - a survey. 05 2020.

[30] Saman Taghavi Zargar, James Joshi, and David Tipper. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE communications surveys & tutorials*, 15(4):2046–2069, 2013.

[31] Dhefaf Radain, Saliha Almalki, Hana Alsaadi, and Shaimaa Salama. A review on defense mechanisms against distributed denial of service (ddos) attacks on cloud computing. In *2021 International Conference of Women in Data Science at Taif University (WiDSTaif)*, pages 1–6. IEEE, 2021.

[32] Rajat Saxena and Somnath Dey. Ddos attack prevention using collaborative approach for cloud computing. *Cluster Computing*, 23(2):1329–1344, 2020.

[33] Junath Naseer Ahamed and N Iyengar. A review on distributed denial of service (ddos) mitigation techniques in cloud computing environment. *International Journal of Security and its Applications*, 10(8):277–294, 2016.

[34] Shui Yu. *Distributed denial of service attack and defense*. Springer, 2014.

[35] Alex Doyal, Justin Zhan, and Huiming Anna Yu. Towards defeating ddos attacks. In *2012 International Conference on Cyber Security*, pages 209–212. IEEE, 2012.

[36] Zhang Chao-Yang. Dos attack analysis and study of new measures to prevent. In *2011 International Conference on Intelligence Science and Information Engineering*, pages 426–429. IEEE, 2011.

[37] U Rahamathullaha and E Karthikeyanb. Distributed denial of service attacks prevention, detection and mitigation–a review. 2021.