https://doi.org/10.29070/n1p50875

A Study the overview of Cloud Computing with its Security Perspectives to Identify Attack

Rashmi M. Chaudhry[1]*, Dr. Pooja Sharma[2]

[1] PhD Student, Department of Computer Sciences Kalinga University, Naya Raipur (C.G.), India

Email: mrashmichaudari@gmail.com

[2] PhD Guide, Department of Computer Sciences Kalinga University, Naya Raipur (C.G.), India

Abstract- Cloud computing has revolutionized how businesses and individuals store, manage, and process data, offering scalable resources and services through the internet. Its flexibility, cost-efficiency, and ease of access have made it an integral component of modern IT infrastructure. However, the widespread adoption of cloud services also brings significant security challenges. This paper provides an overview of cloud computing, outlining its fundamental concepts, service models (IaaS, PaaS, SaaS), and deployment models (public, private, hybrid, community). Several types of attacks threaten cloud systems, including data breaches, denial-of-service (DoS), insider threats, account hijacking, and insecure APIs. These attacks target critical areas such as data confidentiality, integrity, and availability. In response, cloud service providers (CSPs) employ various security mechanisms. This paper emphasizing the need for robust security frameworks to mitigate attacks in the cloud.

Keywords- Cloud Computing, Security, Attacks, DoS, DDoS

- X -

INTRODUCTION

The term "intrusion" describes any effort to breach the security measures put in place to protect a network from potential threats that compromise its confidentiality, integrity, and availability (CIA). Virus invasion boosted data transfer rates. As the most current Intrusion Detection System (IDS) is always evaded, it is clear that intruders are more intelligent than the detector. Identifying traffic involving humans has become a non-trivial issue due to the exponential growth of network traffic. Network IDS capacity to function is dependent on human knowledge. Cloud computing security is an important sub-domain of network security. A suite of rules, apps, methodologies, and the cloud's secure architecture make up cloud security. Customers & businesses of all sizes can take advantage of the storage and processing power of third-party data centers with cloud-based solutions. The main advantages of cloud computing, which are quickly being adopted, include increased efficiency, agility, flexibility, decreased capital expenditure, and the ability to compete on a worldwide scale despite geographical limits. A description of the cloud computing model provided by the National Institute of Standards & Technology (NIST) states that it enables ubiquitous, on-demand services to access a shared pool of configurable technological assets like servers, networks, services, etc., which can be easily provisioned or released with minimal interaction from service providers. While many businesses and organizations are making heavy use of cloud services, many of those same customers are concerned about potential threats to their data.

CLOUD COMPUTING

The term "cloud computing" refers to an approach that allows users to automatically have access to a shared pool of resources regardless of their physical location. Figure 1 depicts the components of the NIST definition of Cloud Computing, which provides a visual representation of the concept.

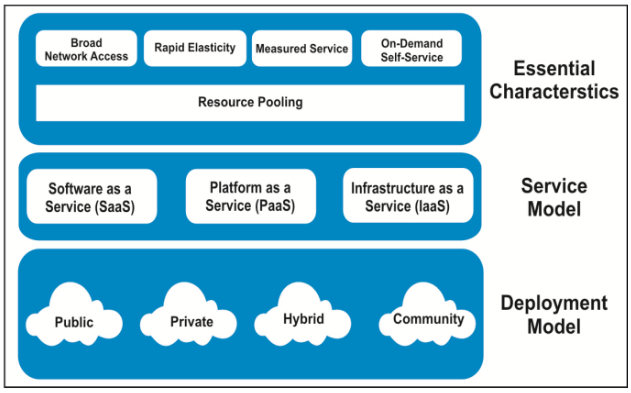

Figure 1 Visualized Definition of Cloud Computing [P. Mell 2011]

One paradigm that has recently emerged is known as "cloud computing," which allows customers to efficiently share the adaptable system resources according to their specific needs. The resources consist of several components such as storage, applications, servers, and services. It requires little effort from management or service providers to be withdrawn or supplied swiftly. With five core features, four deployment methods, and three development or service models, this architecture improves availability. In cloud computing, users have on-demand access to a shared pool of shared computer resources, including data storage, processing power, and other resources, but they don't have direct control over these resources at all times. As a leading example of emerging technology, cloud computing provides Internet users with access to virtualised resources and dynamic scalability.

ARCHITECTURE OF CLOUD COMPUTING

The architecture of Clouds comprises of several loosely coupled components. Front end and back end are the two main components of Cloud architecture, as shown in Figure 2. The front end is the user component that comprises of the tools and applications needed for accessibility to the Cloud Computing systems, for instance, Web Browser. The back end relates to Cloud as a whole and includes every last resource essential to offer services of Cloud Computing.

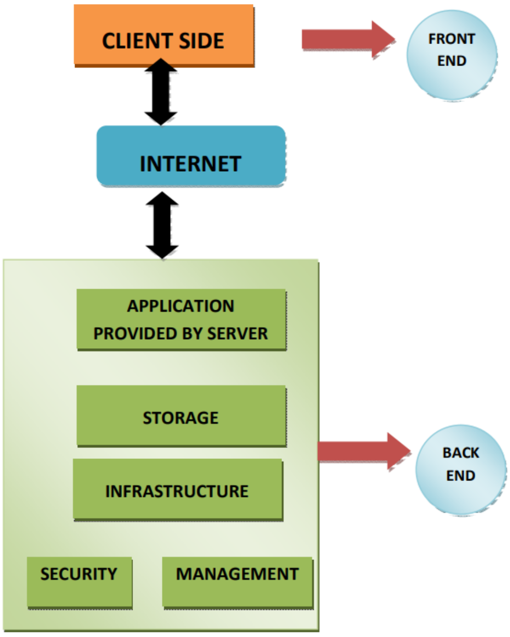

Figure 2 Cloud Architecture

DEPLOYMENT MODELS OF CLOUD COMPUTING

Based on deployment, there are four types of Clouds:

a) **Public Cloud:** In public Clouds services are provided by the third-party providers over the public Internet. These services are accessible to everyone who is willing to utilize or purchase them. The clients can use the services on the basis of pay according to the usage or without payment also. The Cloud provider hosts the infrastructure at its own location. The customers don't have any command and do not bother about where the computing infrastructure is hosted. It can be used by anyone like general public or different organizations.

b) **Private Cloud:** In private Clouds services are provided over the Internet or private network of the organization. It is devoted to a specific organization. The organizations having private Clouds do not share their infrastructure with others. Figure 1.8 shows that there is a physical separation among the clients of a private Cloud. These are more secure but expensive than public Clouds [Tinni Saha 2019].

c) **Hybrid Cloud:** In a hybrid Cloud, any structured technology binds two or more distinct cloud infrastructures around each other. It is a blend of third party public Cloud and on premises private Cloud with orchestration between the two platforms. This empowers data and application accessibility.

d) **Community Cloud:** Only the consumers from an organization which has related concerns can access it. A community Cloud is a collaborative effort where various organizations of a specific community share the infrastructures. The organization itself or a third party can supervise, organize and operate these.

CLOUD COMPUTING DEVELOPMENT MODELS

The three kinds of development or service delivery models of the Cloud are:

i) **Software as a Service (SaaS):** Consumers use Cloud-based applications in the SaaS model supplied by the Cloud supplier [CloudLegals 2018]. With a program interface, clients can use the applications. Consumers need not be concerned about the Cloud's underlying infrastructure. In the data center of the service provider, app software, app information, all the underlying infrastructure, and middleware are situated. Under the terms of an appropriate service contract, the provider not only keeps the hardware and software up and running, but also guarantees that the app and its data are accessible and secure. A common example of SaaS is Email. Figure 1.11 shows the SaaS model of Clouds.

ii) **Platform as a Service (PaaS):** PaaS paradigm has been around for a while and allows businesses to operate apps without the hassle of maintaining their own software & hardware infrastructure.

iii) **Infrastructure as a Service (IaaS):** Infrastructure as a Service (IaaS) in the cloud refers to self-service models that allow users to access, monitor, and manage computing, storage, networking, and other services provided by remote data centres (e.g. firewalls). Computing resources like as storage, networks, processing power, etc. are made available to the client. Any kind of software, including operating systems and applications, may be installed and executed by the client. The client isn't keeping an eye on the bottom-most Cloud base. The client, on the other hand, gets to decide on the operating system, data storage methods, and applications to utilise.

CLOUD COMPUTING: A SECURITY PERSPECTIVE

The Internet remains the core technology of cloud computing, despite the fact that it is a sophisticated technology. Since the Cloud is built on top of the Internet, it is likewise vulnerable to all of the Internet's security risks [D. Puthal 2015]. Cloud computing allows clients and service providers to share resources remotely from various physical locations. As a result, Cloud computing is becoming increasingly vulnerable to cyberattacks. Among the many issues associated with cloud computing, security ranks high because of the geographical dispersion of cloud service providers [M. Ahmed 2014; K. Hashizume 2011]. The advantages of the cloud, such as scalability, dependability, and reduced costs, have led many companies to outsource their IT infrastructure to the cloud. Without a question, organisations are starting to pay more attention to clouds nowadays, but cloud computing is also making them more susceptible to security risks. Cloud security is now receiving increasing attention from boardroom individuals [P. Oberoi 2018]. Despite organisations' growing interest in cloud computing, security concerns remain a major hurdle. The Cloud's open-source, trading, and sharing nature makes it easy for an intruder to circumvent security protocols and safeguards.

The transmission of vital information across the open Internet makes cloud computing an insecure medium. Any setting where computers are used raises concerns about security [I. Kopachevsky 2016]. There are risks to the Clouds from both internal and external sources, including the Internet. Figure 3 shows the three basic properties that determine security: confidentiality, integrity, and availability. When CIA (Confidentiality, Integrity, and Availability) are abused to varying degrees, it compromises the entire framework's security.

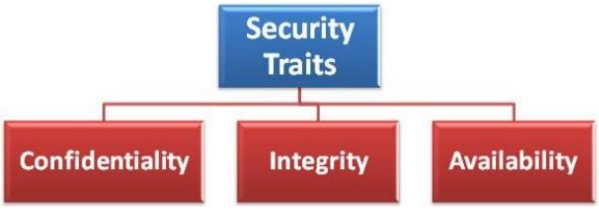

Figure 3 Three Security Traits

The term "threat" refers to anything that might cause damage to the system or for CIA features to be lost [R Madhubala Patil 2015]. Vulnerabilities are holes in the system that malicious actors can use to their advantage. Issues that arise between consumers and providers of Cloud services pose a multitude of concerns. Data that is private & secured against exposure by unauthorised parties is known as confidential. Because data in the cloud is kept on several servers in different physical locations, data privacy is of the utmost importance. If the data can only be accessed by authorised entities, then we say that it has integrity. This means that the data is received exactly as it was transmitted. By preventing unauthorised access, we can increase confidence in the integrity of information and systems. By "availability," we mean the capacity to access data at any time, from any location, and in a protected way; in other words, only authorised users will have access to the data stored on the cloud. Regardless of the severity of a cyberattack, the Cloud servers should continue to function normally. More research into the CIA idea is required for cloud computing, according to M. Babaeizadeh (2015) and Sanzgiri (2002), because cloud servers and the client end both store vital client data.

Authentication is a key component of information security since it guarantees that only authorised individuals may access the data. Path integrity is one of several difficulties in the cloud environment that must be carefully considered. The latter guarantees that the data is accurate, complete, and unaltered. The primary issue with cloud computing is the need to verify the route integrity at an untrusted server. Data must not be altered or deleted without proper authorisation in order to maintain data integrity. According to research by M. S. Giri (2015) and R. Velumadhava Rao (2015), the cloud computing environment's integrity is its most important feature. Due to their lack of direct control over the data, clients run the risk of having their information compromised in some way. Furthermore, there is a physical separation between the clients and the Cloud Server. Because of this, you can't put all your faith on the server to handle user data and access permissions. There is a large range of users with strong leads and regular visits to the Cloud Computing platform. Accordingly, it necessitates a number of safety measures [M. Ali 2015; A. Jain 2017].

Ensuring confidentiality, integrity, and availability (CIA) requires using cutting-edge security measures, effective risk management strategies, and dependable management concepts, all of which work hand in hand with maintaining consensus across security models. Consequently, strong encryption and security mechanisms are essential for cloud computing [U. K. Singh 2014].

The Cloud Security Alliance (CSA 2016) Treacherous 12 – Cloud Computing Top Threats recognized the following 12 critical problems:

a) **Data Breaches:** Cloud Security Alliance (CSA) identified the data breaches as the most severe security threat. The theft of confidential data by an unauthorized person is known as a data breach. For instance, because of the security vulnerability, the Bit defender had to suffer an enormous loss as they lost several usernames and passwords. Malicious user attacks that have the Virtual Machine (VM) on a continuous physical machine can also contribute to a safety violation.

b) **Insufficient Credential, Access, and Identity Management:** These are the novel attacks identified by this study. These attacks result from a loss of multifactor authentication, the use of less stable passwords, the accessibility of access leadership systems to identify the true customer and less convenient automated shifting of keys used for cryptography and certificates. This, in turn, facilitates the attackers in the exfiltration of resources. These attacks may occur due to both; insiders and outsiders attackers. Managing user access control and authentication in private and public Clouds is quite challenging. Procedures for access management and user authentication have been recognized as key components of safety issues.

c) **Insecure APIs and Interfaces:** Clients use application programming interfaces (APIs) and insecure interfaces (IIs) to interact with Cloud facilities. These function as the gateway to assaults and problems related to confidentiality, integrity, accessibility, and accountability. A number of security issues can be lead by weak interfaces, and APIs in Clouds. The Cloud providers provide mostly the APIs as a third party service. This can lead to access to security keys and vital information by third parties [A. Jain 2014].

d) **System Vulnerabilities:** This is another recent menace recognized in this study. These are the bugs that attackers use in the scheme (application or running system) to break into a computer system. This sort of risk is not recent, but Clouds ' cross-tenancy and shared resource and memory capabilities have created a fresh event surface.

e) **Account Hijacking:** In Cloud Computing, account hijacking is more hazardous as malicious intruders can access all Cloud operations by means of the stolen passwords. After obtaining access to the Cloud scheme, the intruder may provide inaccurate data, may monitor transactions and facilities, or may redirect customers to fake websites that may cause providers legal issues.

f) **Malicious Insiders :** A Malicious Insider (MI) such as the system administrator does have full access to the Cloud system as a whole. This assault has an impact on all three designs of Cloud service. The detrimental outcome of this attack is the less of credibility, economic loss, and diminished productivity of the organization. Access to critical systems by malicious insiders begins with IaaS and increases with PaaS to SaaS [P. Mell 2011]. MI is, therefore, more responsible for schemes that depend on CSPs for safety purposes only. Even if the keys are only available when using data, the system is also subject to this attack. There are enthusiast hackers who may be supervisors and steal data for pleasure, and then another kind of insiders are business spies who steal business information [A. Jain 2014].

g) **Advanced Persistent Threats (APTs):** The difficult and ongoing method of spying by individuals contributes to APTs. APTs primary objective is market competition or political expression.

h) **Data Loss:** For any organization, data is the greatest asset if lost can eventually produce terrifying outcomes. In the case of Clouds, the implications can be more drastic.

i) **Insufficient Due Diligence: In** all 14 domains of CSA Security Guidance Reference, this threat has been recognized. The absence of a thorough understanding of the CSP setting makes Clouds more suspectable to various types of assaults.

j) **Cloud Services Abuse and Nefarious use:** All deployment models of Clouds are prone to such an attack. Cloud services such as service paths or designs of poorly guaranteed implementation resulted in malicious assaults. The capacity of the Cloud is diminished by reducing resource accessibility through malicious use. Compared with service users, this attack has severe impacts on service suppliers. For instance, when a malicious person utilizes spam addresses of the Cloud network, it can lead to the blacklisting of address.

k) **Denial of Service:** These assaults restrict customers to Cloud facilities from accessing their accounts. The authorized clients of the Clouds are led to the distressed state because of DDoS assaults, as they don't understand that what the reason for no response from Clouds is? This assault is even worse for clients or users as depending on the cycle and disk, they have to pay.

l) **Shared Technology Vulnerability (STV):** Clouds have a high probability of STV assault due to its sharing nature. Even if it inadvertently or intentionally shares a very tiny piece of critical information, the entire Cloud scheme becomes vulnerable to risks. STV is quite crucial because it affects the entire Cloud at once. The attackers often use STVs to access the Clouds.

However, Clouds offer a number of advantages still they are prone to security threats in general and malicious insiders in particular. The intrusion detection methods used in traditional systems are unable to manage with the needs of the distributed and virtual nature of Clouds.

DENIAL OF SERVICE ATTACKS (DOS)

A denial-of-service attack just requires one computer and an internet connection to overwhelm a server with packets (TCP / UDP). The goal of a distributed denial of service attack is to cause the targeted server to experience resource and bandwidth overload. This will render the server unreachable to all users, thereby barring access to the website or any other content housed on it. Khan C. Smith was the first to demonstrate a denial-of-service attack at a DEF CON event in 1997 by taking down the Las Vegas Strip's Internet service. More over 60 minutes passed during the presentation, during which the attack's sample code was also made public. Throughout the year, the disclosed code was the major cause of internet attacks on E-Trade, EarthLink, and Sprint. Attacks that aim to temporarily or permanently block legitimate users from accessing a service are known as denial of service attacks. Some denial-of-service assaults overwhelm the services, while others bring them to a halt. It should also be taken into account that the most severe assaults are consistently dispersed.

DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS)

There are a lot of similarities to a denial-of-service assault, but the outcomes are drastically different. Distributed denial of service attacks use several computers and internet connections instead of just one. The computers responsible for such an assault are typically part of a larger network called a bot-net, and they are typically located all over the globe. In a DDoS attack, several attackers work together to flood the target server with requests, while in a DoS assault, a single attacker is responsible for the overload. So, a server can't hope to survive a DDoS any more than a regular DoS intrusion.

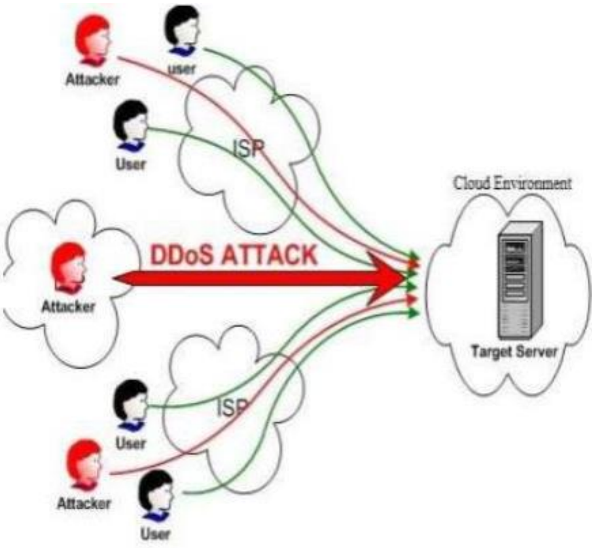

Figure 4 DDoS Attack

One method of launching a DDoS attack is via faking an IP address. Since the incoming attack traffic comes from several sources, filtering systems will not be able to halt the attack. When malicious traffic originates from a large number of different locations, it becomes nearly impossible to differentiate it from normal user traffic. In 2017, the size of distributed denial of service assaults surpassed one terabit per second.

CLASSIFICATION OF DDOS ATTACKS

Distributed denial of service (DDoS) assaults are notoriously difficult to counter or track down because of their distribution. One of the crucial elements in developing an efficient and successful DDoS defensive system is knowing and understanding all the features of DDoS assaults. Rashmi and Kailas (2015) outlined why it's important to learn about distributed denial of service attacks and how they affect cloud environments. In Figure 5, we can see how distributed denial of service attacks are categorised according to their method, flow, impact, and deployment.

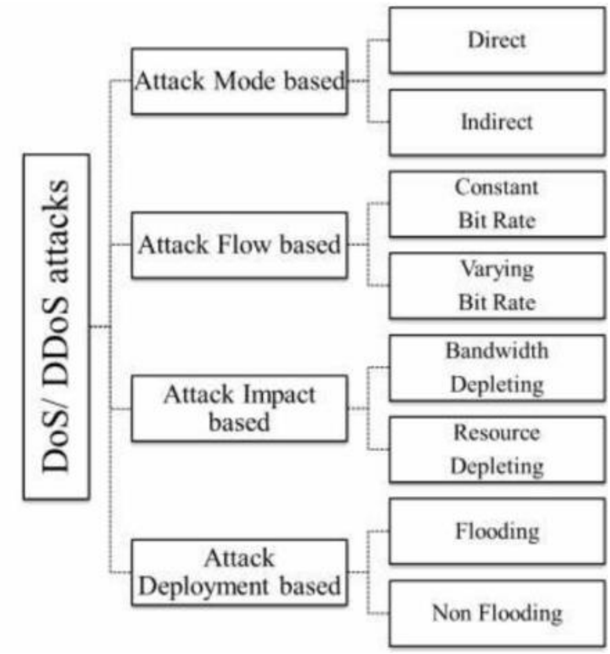

Figure 5 Classification of DoS/DDoS Attacks

There are several forms of DDoS attacks; however, this study just addresses flooding attacks, the most prevalent type of DDoS. An assault that floods the network with undesired packets (either duplicated packets or unique packets sent at a rate higher than the node's rate limit) is known as a flooding attack. There are two main ways that DDoS are categorised here: by the protocol level affected and by botnets. There are two main types of flooding assaults, distinguished by the protocol level. One possibility is at the application level, while the other is at the network/transport level. The majority of attack vectors at the network/transport layer are UDP, TCP, ICMP, and DNS protocol packets. There are four different forms of network/transport level DDoS flooding attacks: normal, reflection-based, protocol exploitation, and amplification based. By depleting the server's resources including sockets, bandwidth, memory, and CPU, application-level flooding attacks aim to disrupt the services of legitimate users. Because they mimic light traffic, these assaults are far more covert than the last one. Asymmetric flooding, reflection/amplification-based flooding, request flooding, and sluggish request/response assaults are subcategories of application level attacks. On the basis of the botnets, distributed denial of service attacks may be classified as either web-based or IRC-based. Based on the criteria given earlier, Figure 6 clearly depicts how DDoS flooding assaults are classified.

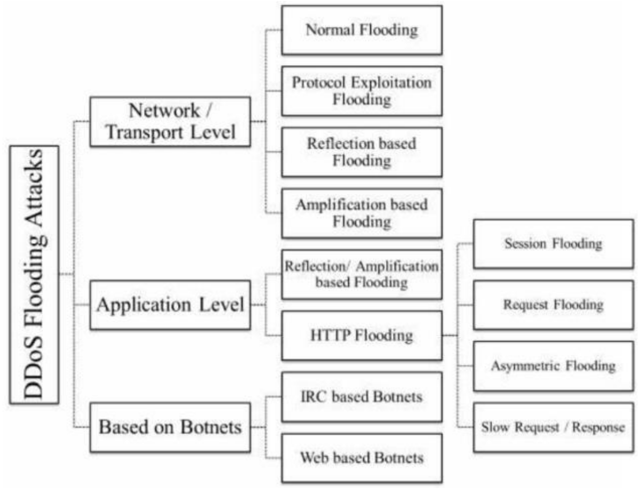

Figure 6 Classification of DDoS Flooding Attacks

NETWORK/ TRANSPORT LEVEL DDOS FLOODING ATTACKS

Packets transmitted via the UDP, TCP, DNS, and ICMP protocols are utilised to launch these types of attacks. This class of attacks includes four distinct kinds.

Normal flooding attacks: Flooding attacks primarily target the connection of genuine users. Attackers aim to use up as much bandwidth as possible on the victim's network. The following protocols and attacks are examples of flooding: UDP, ICMP, DNS, VoIP, etc. Spoofed or non-spoofed IP addresses can accomplish all of these flooding goals.

Attacks that flood protocols with exploits: In these cases, the focus is on the implementation faults of the victim's protocols. The majority of the victim's resources are consumed by attackers because they exploit certain characteristics. Protocol exploitation flooding attacks can take many forms, such as TCP SYN floods, RST/FIN floods, ACK and PUSH ACK floods, and so on.

Reflection-based flooding attacks: Attackers send fraudulent ICMP echo queries to mirrors instead: The reflectors will then communicate back to the victim with their responses. Thus, the victim's resources are depleted by the reflectors. Attacks such as Smurf and Fragile are examples.

Amplification-based flooding attacks: In these attacks, the attackers take use of services to send bigger and more frequent messages to the target, increasing the traffic volume. Botnets are an integral part of any strategy that employs reflection and amplification. An example of an amplification assault would be a smurf attack, in which the attacker takes use of the IP broadcast function of packets to send bogus requests to a large number of reflectors.

Riorey, Inc. (2012) laid out all of the aforementioned forms of assault in great detail. When compared to flooding attacks at the network or transport level, application-level DDoS attacks are more covert. Attacks on the application layer are becoming more common. Application layer distributed denial of service attacks target the OSI models' application layer. In order to temporarily or permanently disable the website or its specialised functionalities, this assault will overuse those functions. Every website has its own unique set of features. Attacks at the network level are rare, despite their apparent potency. There appears to be no halt in the proliferation of attacks aimed at the application layer.

BOTNET-BASED DDOS ATTACKS

When it comes to automating DDoS floods, botnets are the main tool. Modern application layer assaults that are particularly sophisticated use botnets. Hoque et al. (2015) provides a comprehensive review of botnets and botnet-based technologies, including their features, benefits, and drawbacks. A brief overview of the botnet's design and the tools used to launch distributed denial of service (DDoS) flooding attacks will be covered below. It becomes more challenging to design efficient and effective security measures when attackers deploy botnets or zombies. There are primarily two main reasons behind this. The initial move is to use a large swarm of zombies to increase the intensity and reach of the assaults. Secondly, it's obvious that attacker-controlled zombies use a fake IP address, which makes them very hard to track.

A swarm of zombies controlled by an attacker is known as a botnet. The bots or zombies that carry out the attacker's commands are called agents, while the botnet itself is called the master. The handlers in botnets facilitate master-agent communication and control by acting as go-betweens for the agents. A common characteristic of compromised networks is the presence of handler software on infected devices. Antivirus software has evolved to the point where it can detect installed programs by analysing their unique digital footprints. Internet Relay Chat is now the method that attackers use to manipulate their bots. Systems that will attack the victim are really compromised bots that their masters control. Figure 7 shows the characteristics of a botnet during a distributed denial of service attack.

Botnets may be deployed in several ways. The presentation by Alomari et al. (2012) suggests that there are three main forms of botnets: IRC, Web, and P2P. The way bots are controlled by their owners determines the kind. Here we break down the two most popular types and show you some instances of the tools used for each.

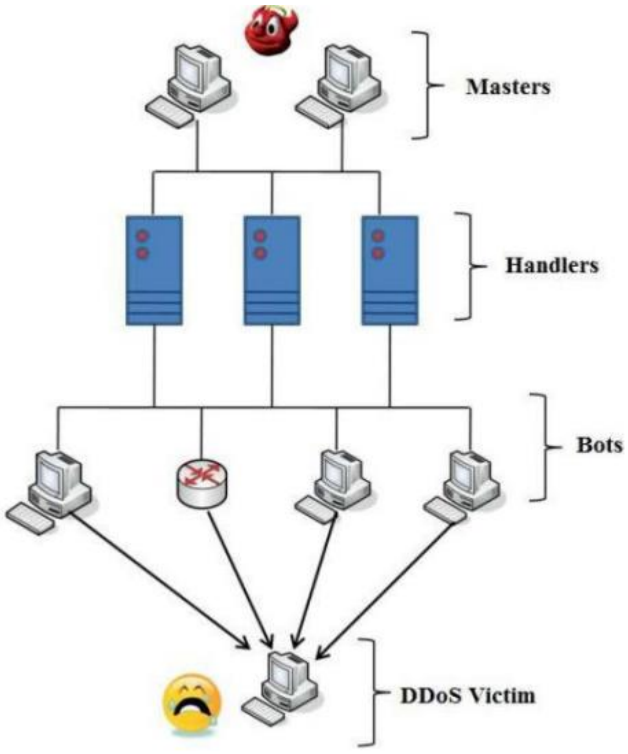

Figure 7 Botnet based DDoS Attack

IRC-based Botnets: Internet Relay Chat is a text-based system for internet instant chat. It can link thousands of customers via several servers and features a client-server architecture. An attacker can command bots using valid IRC ports by taking use of IRC channels as handlers. Since there is usually a lot of activity on IRC servers, it's easy for an attacker to hide and spread malware through file sharing. By login onto the IRC server, attackers may view the list of all accessible bots, rather than keeping a list locally at their site. IRC botnets rely on a centralised command and control (C&C) infrastructure, which has one big drawback: servers might be a single point of failure. The elimination of the botnet is possible if the defender manages to seize control and command servers. Trinity v3 and Kaiten are two popular botnets that use IRC to perform distributed denial of service attacks. One of Trinity v3's well-known features is its ability to execute UDP flood attacks, while another is Kaiten's reputation for successfully executing TCP SYN, ACK, NUL, & PUSH+ACK assaults.

Web-based Botnets: The term "HTTP based botnet" describes a botnet in which the command-and-control messages are sent via the HTTP. The use of HTTP for communication makes it more difficult to trace back to the command-and-control structure. In contrast to botnets that rely on Internet Relay Chat (IRC), web-based botnets don't keep in touch with a central server; instead, each web bot periodically uses web requests to obtain the instructions. When communicating with web-based bots, complex PHP scripts encrypt data sent over the HTTP (port 80) or HTTPS (port 443) protocols.

Because they can blend in with real HTTP traffic, web-based botnets are inherently more stealthy than botnets based on IRC. Three popular and extensively utilised web-based botnet programs are BlackEnergy, Low-Orbit Tonne Cannon (LOIC) 4, and Aldi. Whenever necessary, the tool's destructive capabilities may wipe out the infected hosts by corrupting all of the data on the hard disc.

CONCLUSION

In conclusion, cloud computing offers immense benefits in terms of scalability, cost-effectiveness, and flexibility, making it a critical technology in the digital transformation of businesses. However, the adoption of cloud services also introduces new security risks and attack vectors that must be carefully managed. The shared, multi-tenant nature of cloud infrastructures makes them susceptible to various attacks, including data breaches, insider threats, DoS attacks, and insecure APIs. While cloud service providers implement a range of security measures such as encryption, identity management, and network protection, these efforts must be continuously updated to counter evolving threats. Additionally, collaboration between cloud providers and users is essential for securing sensitive data and maintaining the integrity and availability of services.

REFERENCES

1. Alomari, E. S. Manickam. B. Gupta, S. Karuppayah, and R. Alfaris (2012). Botnet-based distributed denial of service (ddos) attacks on web servers: classification and art. arXiv preprint arXiv:1208.0403.
2. Attou, H., Guezzaz, A., Benkirane, S., Azrour, M., & Farhaoui, Y. (2023). Cloud-based intrusion detection approach using machine learning techniques. *Big Data Mining and Analytics*, *6*(3), 311-320.
3. Bhange, A., Syad, A., & Thakur, S. S. (2012). DDoS attacks impact on network traffic and its detection approach. *International Journal of Computer Applications*, *40*(11), 36-40.
4. Carlin, A., M. Hammoudeh. and O. Aldabbas (2015). Defence for distributed denial of service attacks in cloud computing. Procedia Computer Science, 73, 490-497.
5. Dadkhah, M., M. D. Jazi, M. S. Mobarakeh, S. Shamshirband, X. Wang, and S. Raste (2016). An overview of phishing attacks and their detection techniques. International Journal of Internet Protocol Technology, %(4), 187195,
6. FuiFui Wong & Cheng Xiang Tan 2014 'A survey of trends in massive DDoS attacks and cloud-based mitigations" International Journal of Network Security & Its Applications (IINSA), Vol.6, No.3.
7. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Comput. Soc., pp. 69–73, 2012.
8. Masdari, M., & Jalali, M. (2016). A survey and taxonomy of DoS attacks in cloud computing. *Security and Communication Networks*, *9*(16), 3724-3751.
9. P. Oberoi and S. Mittal, "Survey of various security attacks in clouds based environments," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 976, pp. 405–410, 2017.
10. Somani, G., M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya (2017). Ddos attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, 30-48.
11. Van Trung, P.. T. T. Huong, D. Van Tuyen. D. M. Duc, N. H. Thanh, and A. Marshall, A multi-criteria-based ddos-attack prevention solution using software defined networking. In Advanced Technologies for Communications (ATC), 2015 International Conference on. IEEE, 2015.
12. Xiao, Z. and Y. Xiao (2013). Security and privacy in cloud computing. IEEE Conmmunications Surveys & Tutorials, 15(2), 843-859.

Corresponding Author

Rashmi M. Chaudhry*

PhD Student, Department of Computer Sciences Kalinga University, Naya Raipur (C.G.), India

Email: mrashmichaudari@gmail.com