# CHAPTER ONE

# INTRODUCTION

## 1.1 Background of the Study

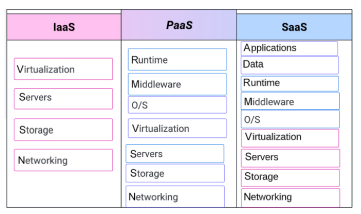
Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP’s) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. Cloud computing is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider’s interaction. In general cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis. In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers (Kundu, Banerjee, & Saha, 2010)

Figure 1: Cloud computing services models (Attou, Guezzaz, Benkirane, Azrour, & Farhaoui, 2022)

A model for providing on-demand computing resources with the least amount of work and maintenance is called cloud computing (Alashhab, Anbar, Singh, Hasbullah, Jain, & Al-Amiedy, 2022). It involves the internet-based sharing of computer resources. Software, a developer interface, virtual hardware, or storage are all examples of these shared resources. A potential paradigm known as "cloud computing" uses the internet to provide software, platforms, and infrastructure as a service that is entirely virtual and does not depend on local computers or memory requirements. In addition to the widely acknowledged offerings and advantages, cloud computing may also provide risks and obstacles (Khalaf, Mostafa, Mustapha, Mohammed, & Abduallah, 2019).

Infrastructure and services are made available "on-need" through the use of cloud computing. More specifically, network-enabled, scalable, assured Quality of Service (QoS), low-cost computing infrastructure, and simple accessibility are all included in cloud computing. Moreover, the industrial cloud computing is becoming increasingly popular as more and more consumers move their data and applications to a remote cloud. Consumers get more flexible access to the data and applications (Alashhab, Anbar, Singh, Hasbullah, Jain, & Al-Amiedy, 2022)

The cloud provides services with high performance due to its characteristics (Singh & Chatterjee, 2017) according to the National Institute of Standards and Technology (Verma & Kaushal, 2011): network access, resource pooling, quick elasticity, and measured service. Recently, the cloud suffers from many security problems like availability, data confidentiality, integrity, and control authorization. In addition, the Internet is used to facilitate access to the services offered by the cloud representing a major source of threats that can infect the cloud systems and resources (Singh & Chatterjee, 2017). Then enhancing cloud security becomes a primary challenge for cloud providers (Alloussi, Laila, & Sekkaki, 2012). Therefore, several approaches such as firewall tools, data encryption algorithms, authentication protocols, and others have been developed to better secure cloud environments from various attacks (Gu, Wang, Wang, & Wang, 2019). However, traditional systems are not sufficient to secure cloud services from different limits (Chiba, Abghour, Moussaid, Omri, & Rida, 2016)

## 1.2 Aim and Objectives

### 1.2.1 Aim

The aim of this dissertation is to develop a cloud computing protection system that utilizes artificial intelligence techniques to enhance the security and privacy of cloud-based systems. The system will leverage machine learning algorithms to detect and mitigate various security threats, as unauthorized access, data breaches, malware attacks, and insider threats. To provide a cloud security model that secures cloud users’ data from unauthorized entity and makes it available at when needed by the rightful owner using deep learning.

### 1.2.2 Objectives

The objective of this research is to secure cloud services for users from computer intruders and raise alarm whenever it happens in order to achieve the following:

1. Design and implement a scalable and robust cloud computing protection system.
2. Develop machine learning models to detect and prevent security threats in real-time.
3. Enhance the security and privacy of data stored in the cloud.
4. Provide intelligent monitoring and response capabilities to ensure continuous protection.
5. Improve the overall performance and efficiency of cloud computing systems.
6. Confidentiality, Integrity and Availability of users’ data.

## 1.3 Statement of the Problem

Cloud users are becoming more and more with their valuable data residing on cloud, a lot of models have been developed to guarantee safety of these valuables but cloud computing intruders are making these models vulnerable.

## 1.4 Significance of the Study

This dissertation describes the development of a new and accurately secured model to solve the problem mentioned in the 1.3 above using deep learning.

## 1.5 Scope of the Study

The scope of this research is limited to small range of data at a start in order to accurately measure its performance and this would lead us to the upgrade of which it can be measured with big data.

## 1.6 Operational Definition of Terms

**Deep learning:** is like machine learning—in fact, it’s more of an application of machine learning that imitates the workings of the human brain. Deep learning networks interpret big data (data that is too large to fit on a single computer) both unstructured and structured and recognize patterns.

**Cloud:** is **a distributed collection of servers that host software and infrastructure, and it is accessed** over the Internet. The cloud is not a physical entity, but instead is a vast network of remote servers around the globe which are hooked together and meant to operate as a single ecosystem.

**Cloud Computing**:  is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale.

**Cryptography**:  is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.

**Security**: is the state of being or feeling secure; freedom from fear, anxiety, danger, doubt, etc.; state or sense of safety or certainty

**Computer Security:** Computer security, cyber security, digital security or information technology security (IT security) is the protection of [computer systems](https://en.wikipedia.org/wiki/Computer_system) and [networks](https://en.wikipedia.org/wiki/Computer_network) from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to [hardware](https://en.wikipedia.org/wiki/Computer_hardware), [software](https://en.wikipedia.org/wiki/Software), or [data](https://en.wikipedia.org/wiki/Data_(computing)), as well as from the [disruption](https://en.wikipedia.org/wiki/Denial-of-service_attack) or misdirection of the services they provide.

# CHAPTER TWO

# LITERATURE REVIEW

## 2.1 Cloud Computing

### 2.1.1 History and Evolution of Cloud Computing

Evolution of cloud computing can be mapped back to older systems which have been used in the real-time long before cloud computing has come into existence. In “Cloud Computing”, the word “Cloud” means carrier or provider who provides the services over the Internet. “Computing” is the processing or computations or calculations or various resources that are provided by computer. The concept of cloud computing traces back to 1961 by John McCarthy at MIT: “If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry” (Garfinkel, 1999).

One of the first companies to start working with the concept of the “cloud computing” is formed by Salesforce in late 1990 (Salesforce, 2019). The company started providing their Software as a Service (SaaS), which provides customer relationship management for its users. Salesforce model is one of the typical patterns of cloud computing, in addition to “Platform as a Service” (PaaS), which provides customers with development platform such as Microsoft Azure (Microsoft, 2019) and Google’s Application Engine (Google, 2019). The other form is “Infrastructure as a Service” (IaaS) model such as Amazon Elastic Compute Cloud (EC2) started in 2006 (Amazon, 2019).

In 2007, many of the US universities started collaborating with Google and IBM and promoted cloud computing programs at their universities. This helped reduce the cost for academic research, sharing the resources between the students, and to build substantial processing power or computing power to access it over the Internet. Many more universities around the globe followed the same trend during the subsequent years (Sultan, 2010).

In July 2010, NASA and Rackspace started a joint project called OpenStack with several vendors including AMD, Intel, and Dell. Later on, many other organizations have joined the project. A non-profit organization called OpenStack Foundation is formed in September 2012 to promote OpenStack (Sell, 2019). Now more than 500 companies are supporting the project (Openstack, 2019). Around 6800 companies are using OpenStack to deploy their cloud services (iDatalabs, 2019).

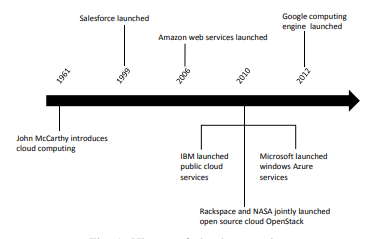
In October 2011, Trusted Cloud Initiative by Cloud Security Alliance (CSA) published a white paper to help cloud service providers to develop cloud services that meet the requirement for industry standards, secure, access controllable, interoperable, and manageable (Orea, J, 2011). Fig. 1 shows the history of cloud computing.

Figure 2: History of Cloud Computing

## 2.2 Cloud Threats

Cloud Computing is a term with substantial and widespread planned improvement. However, as stated below (Kshirsagar & Akojwar, 2016), it has different risks to safety and protection issues. The analysis is based on the CIA feature and cloud threats.

### 2.2.1 Cloud Security Threats

CC has classified the key vulnerabilities are confidentiality, integrity, authenticity, and availability as illustrated in **figure 3**. These concerns are briefly addressed below

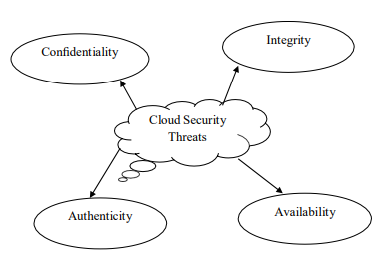


Figure 3: Cloud security threats

1. Confidentiality threats: It contains internal threats to client records, the danger of foreign threats, and software problems.
2. First, an intruder threat to customer data is due to unauthorized or an unapproved user to personal information by an intruder of a cloud service provider is a substantial protection threat (Seitz, Selander, Wahlstroem, Erdtman, & Tschofenig, 2019).
3. Second, for cloud systems in unprotected areas, the possibility of external attacks is highly prevalent. This possibility involves centralized cloud and web services device or hardware (Kshirsagar & Akojwar, 2015).
4. Third, data loss is an unrestricted vulnerability of cloud negotiation details caused by human errors, lack of tools, and access failures, whenever feasible.
5. Integrity threats: This includes risks to the division of records, inadequate regulation of customer access, and vulnerability to the level of data.
   1. First, the possibility of exclusion from details inexactly linked to protection criteria poorly informed architecture of VMs, and off-base virtual servers on the part of customers. This is a complex cloud problem that provides customer connections; changes in assets may impact the reliability of data (Kshirsagar & Akojwar, 2016).
   2. Secondly, poor management of clients' access, with numerous problems and threatening factors which allow attackers to damage data assets due to lack of proper influence and sharing of personality
6. Authenticity threats: The authentication mechanism ensures that the equipment and related is initial and trustworthy. For instance, patient criteria are sent to various treatment centers within the medical and health system. If this information is handled and obtained by an attacker, the therapy of the patient will be problematic.
7. Availability threats: It includes Risks to transparency, the effects of panel growth, inaccessibility of organizations, external disruption of equipment, and improper recovery strategies.
8. Firstly, emphasis has been placed on the board which includes the impact of the entry into test customers for various customers and the result of adjustments to the foundation (Khan & Herrmann, 2019). The usability of cloud organizations is adversely affected both by infrastructure and effects ranging in the cloud condition (Zhou & Lopez, 2013).
   1. Secondly, the failure to access systems that include the inaccessibility of device data transmission, domain name system (DNS) applications, and properties. An external risk affecting all versions of the cloud (Kshirsagar & Akojwar, 2015).
   2. Thirdly, the IT services suppliers, cloud users, and a large network (WAN) specialist institution are physically disrupted.
   3. Fourthly, weak strategies of recovery, including poor recovery from failures which affect retrieval time and efficiency if a stage occurs.

### 2.2.2 Attacks on the Cloud

Four comparative threats are classified according to their fragments: network-based, VM-based, storage-based, and application-based as depicted in Figure 4.

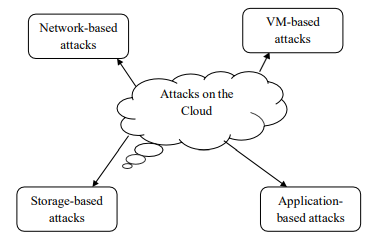


Figure 4: Attacks on Cloud

1. Network-based attacks: Port checks, botnets, and spoofing threats are three examples of device attacks explored. A vulnerability scanner helps hackers to evaluate the intruder to gather necessary details to initiate an attack (Seitz, Selander, Wahlstroem, Erdtman, & Tschofenig, 2019). Depending on the regular routes of a network's protection, the security normally doesn't conceal their identities as the hackers check the network (Thamilarasu & Chawla, 2019). A botnet is an advancement in web-related malicious polluted computers that attackers can penetrate. An attack of spoofing occurs when an attacker or fraudulent program successfully works with imitating information on behalf of an individual user (or system). This takes place when the hacker claims to be somebody (or another computer, such as a telephone) and uses a network to control or give away confidential data from other computers, devices, or individuals (Khan & Herrmann, 2019).
2. VM-based attacks: Various systems-enabled VMs trigger several security concerns. A side-channel attack is an interference dependent on information from the program execution of the machine instead of defects in the software (Zhou & Lopez, 2013). When the VM is created, malicious software inserted within the VM image is repeated. VMs display the architecture of the Executive for the recognition and retrieval of safety risks, splitting, and filtering.
3. Storage-based attacks: Astringent surveillance process is not taken into account as hackers hack key stored data on such storage devices. The data scrounging means that an intruder can't view or restore this data entirely from storage devices. The synchronous replication of data applies to replicate data copies (Rachapudi, Nitish, Samaikya, Sathvik, & Devi, 2020). This threat is remedied by making sure that the exact number of copies of the file is doubled.
4. Application-based attacks: The software program in the cloud will confront numerous attackers which influence its efficiency and trigger suspicious data leakage. Malware explosion and stenography attacks, popular architectures, online servers, and symposium threats are the three main app-based threats (Anjali, Sapkota, Rohit, Pooja, & Sandeep, 2020).

## 2.3 CLOUD COMPUTING BUILDING BLOCKS

### 2.3.1 Models of cloud computing

Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

1. **Software-as-a-Service (SaaS)**: SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support (Grossman, 2009). SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data center space, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. SaaS features a complete application offered as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps (Padhy, R P; Patra, M R; Satapathy, S C;, 2011).

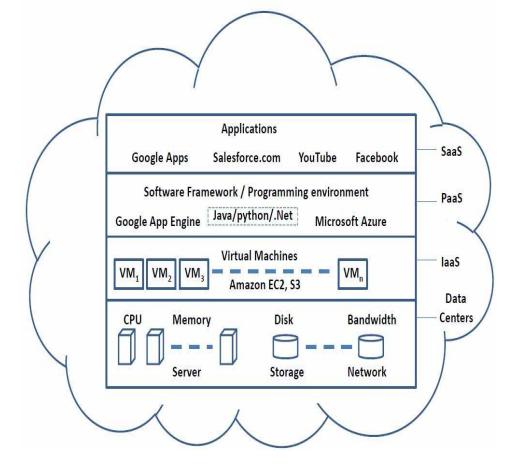


Figure 5: High Level View of Cloud Computing Architecture

1. **Platform as a Service (PaaS):** “PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure (Padhy, R P; Patra, M R; Satapathy, S C;, 2011).
2. **Infrastructure as a Service (IaaS)**: Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS include Amazon Elastic Cloud Computing (EC2), Amazon S3, and GoGrid.

### 2.3.2 Cloud deployment models

There are also four different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below.

1. **Private cloud**: Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user’s access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems (Kandukuri, Paturi, & Rakshit, 2009).
2. **Public Cloud**: A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud include Microsoft Azure, Google App Engine.
3. **Hybrid Cloud**: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services (Jensen, Schwenk, Gruschka, & Iacon, 2009). A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).
4. **Community Cloud**: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook which is showing in **figure 3**

**Cloud Deployment Models**

### Deployment model.PNG

Figure 6: Cloud deployment models (Butt, et al., 2020)

### 2.3.3 Cloud computing entities

Cloud providers and consumers are the two main entities in the business market. But, service brokers and resellers are the two more emerging service level entities in the Cloud world. These are discussed as follows:

**Cloud Providers**: Includes Internet service providers, telecommunications companies, and large business process outsourcers that provide either the media (Internet connections) or infrastructure (hosted data centers) that enable consumers to access cloud services. Service providers may also include systems integrators that build and support data centers hosting private clouds and they offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers (Pring et al, 2009).

**Cloud Resellers**: Resellers can become an important factor of the Cloud market when the Cloud providers will expand their business across continents. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as “resellers” for their Cloud-based products in a particular region. Cloud Consumers: End users belong to the category of Cloud consumers. However, also Cloud service brokers and resellers can belong to this category as soon as they are customers of another Cloud provider, broker or reseller. In the next section, key benefits of and possible threats and risks for Cloud Computing are listed (Bakshi & Dujodwala, 2010).

## 2.4 Cloud Computing: Security Issues and Research Challenges.

Cloud computing is an architecture for providing computing service via the internet on demand and pay per user access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate (Padhy, R P; Patra, M R; Satapathy, S C;, 2011).

## 2.5 Allocating Duplicate Copies for Internet of Thing (IoT) Data in Cloud Computing Based on Harmony Search Algorithm

(Jahandideh & Mirzaei, 2022) As two entirely distinct technologies, Internet of Thing (IoT) and cloud computing have complementary features that evolve rapidly. In fact, the IoT benefits from the unlimited storage and processing power of clouds, and in return, cloud computing can take advantage of the IoT features to provide more distributed and dynamic communications with real-world objects. Cloud computing focuses mainly on the development of powerful data centers to provide end-users with dynamic and flexible services (Shao, Li, & Tang, 2019). Therefore, when the IoT transmits the data sensed by wireless sensors to the cloud for storage, multiple replicas of the transmitted data are stored in the cloud so that the data can be sent from the closer server to the end-user upon request. The replicas of IoT data are stored in the cloud computing environment to retain data and prevent data deletion and loss in the cloud and also accelerate the end-users access to data. Since heuristic methods operate slowly in selecting data centers for data replication, meta-heuristic methods can be a better alternative choice (Mansouri & Javidi, 2020). Accordingly, this paper employed the HS algorithm to propose an approach to the allocation of IoT data replicas in the cloud computing environment. The HS algorithm was used because the proposed approach can properly benefit from its advantages in both local and global search procedures, thus covering the weaknesses of other existing methods. Inspired by music, the HS algorithm aims to reach the best solution through coordination and harmony. The attempt at finding harmony and coordination in music resembles the discovery of optimal conditions in an optimization process.

## 2.6 Recent Trends on Sophisticated types of Flooding Attacks and Detection Methods based on Multi Sensors Fusion Data for Cloud Computing Systems

(Alhammadi, Mabrouk, & Zrigui, 2022) The management, processing, access, and storage of information and other data within a specific server are known as cloud computing (Parast, Sindhav, Nikam, Yekta, Kent, & Hakak, 2022). Infrastructure and services are made available "on-need" through the use of cloud computing. More specifically, network-enabled, scalable, assured Quality of Service (QoS), low-cost computing infrastructure, and simple accessibility are all included in cloud computing. Moreover, the industrial cloud computing is becoming increasingly popular as more and more consumers move their data and applications to a remote cloud. Consumers get more flexible access to the data and applications (Alashhab, Anbar, Singh, Hasbullah, Jain, & Al-Amiedy, 2022). Although cloud computing has many advantages, it is still in early stages and faces numerous hurdles in terms of integrity, security, availability, cost, and performance. The biggest challenge in cloud computing is security because many people find it intimidating to use someone else's harddrive to store or operate software (Agrawal & Tapaswi, 2019). A model for providing on-demand computing resources with the least amount of work and maintenance is called cloud computing (Alashhab, Anbar, Singh, Hasbullah, Jain, & Al-Amiedy, 2022). It involves the internet-based sharing of computer resources. Software, a developer interface, virtual hardware, or storage are all examples of these shared resources. A potential paradigm known as "cloud computing" uses the internet to provide software, platforms, and infrastructure as a service that is entirely virtual and does not depend on local computers or memory requirements.

Security experts have been making great efforts to report this problem for a while, but the frequency and impact of these attacks have increased despite their efforts. As a result, it is urgently necessary to incorporate the concepts of adaptation and self-organization into the design of effective cloud security measures. Distributed Denial-of-service (DDoS) attacks, however, can be launched from a variety of contexts, including a specific service, cluster, node, virtual machine or the entire cloud environment. When an attacker uses numerous zombie machines that are already under their control to transmit a large number of false packets from one direction to a server, DDoS happens (Khan, Khaleel, & Daghighi, 2021). DDoS attacks have grown to be a significant issue, and attackers are now focusing on victims in sophisticated ways.

Nevertheless, Infrastructure as a whole has become a frequent target for attacks due to the widespread usage of virtualization technology. In particular, privilege escalation and Denial of Service (DoS) attacks (Lata & Singh, 2022). The dilemma of availability in cloud security is seriously threatened by DoS attacks. DoS attacks have a higher potential in cloud computing than they do in single tenanted architecture because millions of users share their infrastructure. There are two ways that DoS attacks can be deployed across the Internet. The first strategy entails the attacker delivering the victim malicious packets in an effort to confuse any program or protocol that is using it (i.e., a vulnerability attack) (Elzamly & Hussin, 2016). Whereas, the second case can be done at the level of transport and application layer. The attacker attempts to consume the network resource and prevent the legitimate user to access to the network (Guha, Yau, & Buduru, 2016). Moreover, the architecture of DDoS on a cloud server was displayed in bellow Figure 7

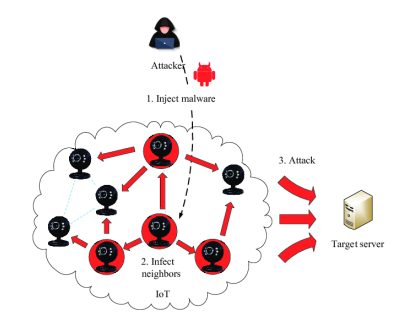


Figure 7: The architecture of DDoS attack on cloud server (Guha, Yau, & Buduru, 2016)

# CHAPTER THREE

# MATERIALS AND METHODS