OPEN ACCESS

Kashf Journal of Multidisciplinary Research
Vol: 01 - Issue 12 (2024)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

SECURITY THREATS AND COUNTERMEASURES IN CLOUD

*Shumaila Iqbal**
Zeeshan Ahmad
Warda Naeem
Muhammad Obaid Ullah
Dr. Muhammad Azam

Department of Computer Science, Superior University Lahore, Pakistan
CORRESPONDING AUTHOR: Shumaila Iqbal (email: su92-mscsw-s23-006@superior.edu.pk)

DOI: https://doi.org/10.71146/kjmr174

Article Info

Abstract

Cloud computing refers to the continuous availability of computer infrastructure technology, enabling the handling and storage of information without direct client management. People are given the ability to access private as well as public information preservation on a single digital infrastructure via the use of the Internet. However, this convenience comes with certain security issues and risks, which have led to the widespread adoption of cloud-dependent computing models. This research delves into various security problems, challenges, methods, and perspectives in one comprehensive article. In addition, a number of upcoming technologies, are dependent on services related to cloud computing to process and store their data. As a consequence of this, a variety of enterprises are expanding their utilization of these technologies, which in turn exacerbates the weaknesses and security challenges inherent to the cloud model. The term "cloud computing" refers to an approach that incorporates all of its constituent parts, such as end users, connections, access management systems, and infrastructures. If security teams do not have a comprehensive grasp of the architecture of the cloud, they might run into problems such as the sluggish identification of security threats, the resulting duplication of data, and a loss of control over accessing the information and protection in order to maintain regulatory compliance. The article begins by briefly introducing the architecture of cloud computing, highlighting its key features, service models, deployment methods, and cloud server virtualization. This paper's primary findings include the growing popularity of cloud computing, security challenges in cloud computing, the importance of investigating security challenges, categorizing security challenges, and proposing developing solutions. Through an extensive review, it analyzes and summarizes scholarly efforts to address these security concerns, followed by information on cloud computing safety concerns and frameworks. Understanding security challenges, addressing data migration challenges, improving security measures, offering a systematic approach, enabling risk detection and prevention, and facilitating the development of preventive methods are the primary significance of this work. The text then categorizes various cloud attacks and privacy issues, before outlining the literature's efforts to provide mitigation and protection mechanisms for security assessment. Finally, it examines unresolved cloud security challenges and proposes potential solutions..

Keywords: *Cloud computing, Security challenges, Data storage, Infrastructure, Access management, Risk detection.*

Introduction

Computing in the cloud is an area of fast developing technology for computers that permits the development of information technology services in a manner that is both affordable and accessible. It is anticipated that the market would reach an astounding $623.3 billion in the year following 2023.(Gudapati Syam Prasad and S. Gaikwad, 2018)

Major IT companies like Amazon, Microsoft, Google, IBM, and Oracle host cloud deployments, providing solutions to various businesses and organizations. Strategies like database grids and distributed database management systems have been implemented to optimize resource usage.This kind of processing may be done online, and it gives users accessibility to a public pool of computer resources from any location and at any time.

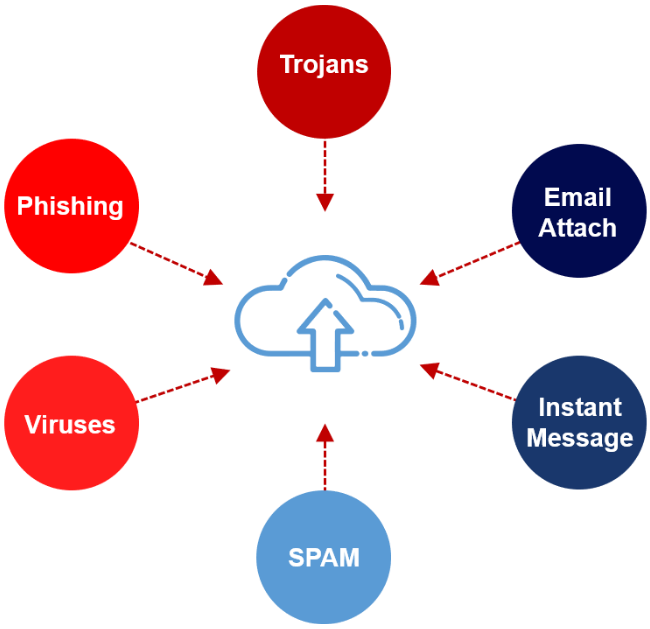

Figure 1: Cloud security threats

It also has a large capacity for processing. Users are able to make any necessary adjustments to their resource demands and are only required to pay for the assets they actually use, hence reducing the amount of financial strain they are under. (Anjana and Singh, 2019)
(*Discover the Cloud Security Threats in 2018 - Cisco Community*, no date)
Cloud-based information technology systems have improved scalability and flexibility, as well as the potential to save money, making them the architecture of choice for enterprises that work in the information technology industry. Amidst the current financial crisis and growing computing demands, the cloud is considered the optimal solution due to its efficient storage and versatile capabilities. This study investigates several facets of a cloud computation, particularly its architectural design, service models, deployment strategies, and potential security risks. It is addressed various service models, such as both private andpublic society as a whole and mixed deployments, as well as IaaS, SaaS, and PaaS.

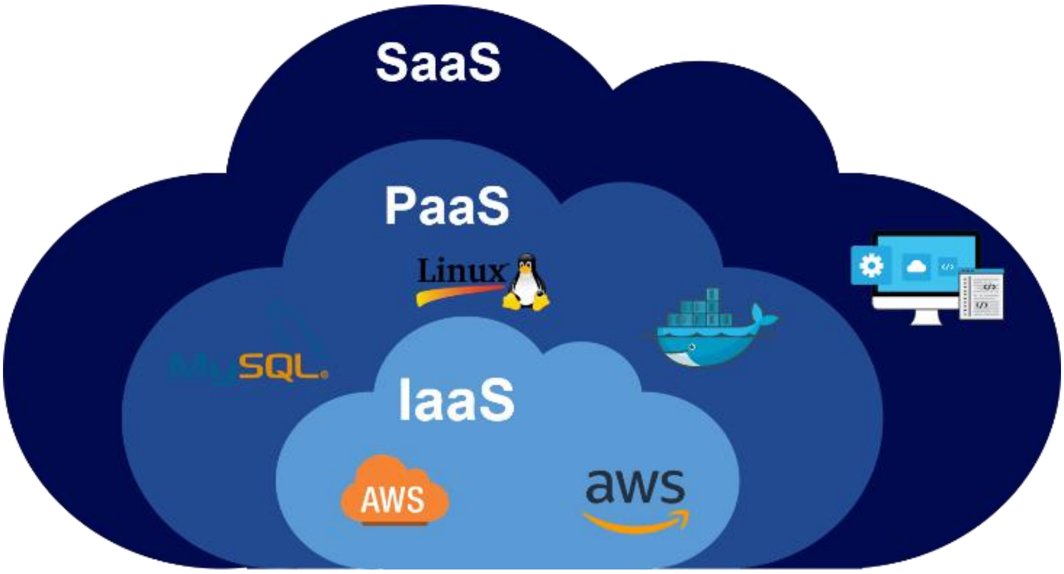

Figure 2: Cloud System and its Phases

The research paper on cloud computing presents a comprehensive analysis, beginning with an introduction to the basic concept of cloud computing in Section 1. Section 2 provides a detailed overview of the background research associated with the field, setting the context for subsequent discussions. Moving forward, Section 3 , scrutinize the identified threats, dangers, and security hazards within the cloud computing environment. The subsequent section 4 further scrutinize the specific vulnerabilities and flaws within the cloud infrastructure, while also outlining the security methods employed to fortify the cloud environment. In Section 5, potential solutions and strategies to mitigate these security challenges are thoroughly examined and proposed. Section 6 emphasizes the importance of establishing a secure cloud processing environment through the implementation of trusted cloud computing practices. Furthermore, Section 7 addresses the critical issue of regulatory compliance in cloud security. Section 8 provides an insightful discussion on the complexities and hurdles related to ensuring robust security in cloud computing. Section 9 further scrutinize the specific vulnerabilities and flaws within the cloud infrastructure, while also outlining the security methods employed to fortify the cloud environment. Finally, the article concludes in Section 10, offering a comprehensive summary of the various security risks and their implications within the sphere of cloud computing.(Khoda Parast *et al.*, 2022)

The various security risks that people using cloud services might encounter. These risks can originate both from within the system and from external sources. As a result, the duty for guaranteeing the safety of essential software and systems lies not only with the consumers of cloud computing, but also with the businesses that provide cloud services and the third-party vendors that are engaged.(*Internet of Things: Security Vulnerabilities and Countermeasures - IOPscience*, no date) Users who make use of cloud services are burdened with the responsibility of protecting their particular applications, while the online computing service supplier in question is responsible for guaranteeing there that they comply with external firewall regulations and the physical security of the infrastructure. In addition, both the customer and the company managing the cloud service share the responsibility of maintaining the safety of the system. Nonetheless, the cloud presents specific security challenges that require the attention of cloud providers to prevent criminal activities and hacker-induced denial-of-service attacks. Many businesses make use of data centers for cloud virtualization, which introduces further security challenges. While virtualization offers advantages such as role-based access and simplified deployment across multiple platforms, it also exposes vulnerabilities that attackers might exploit, leading to potential threats and attacks.

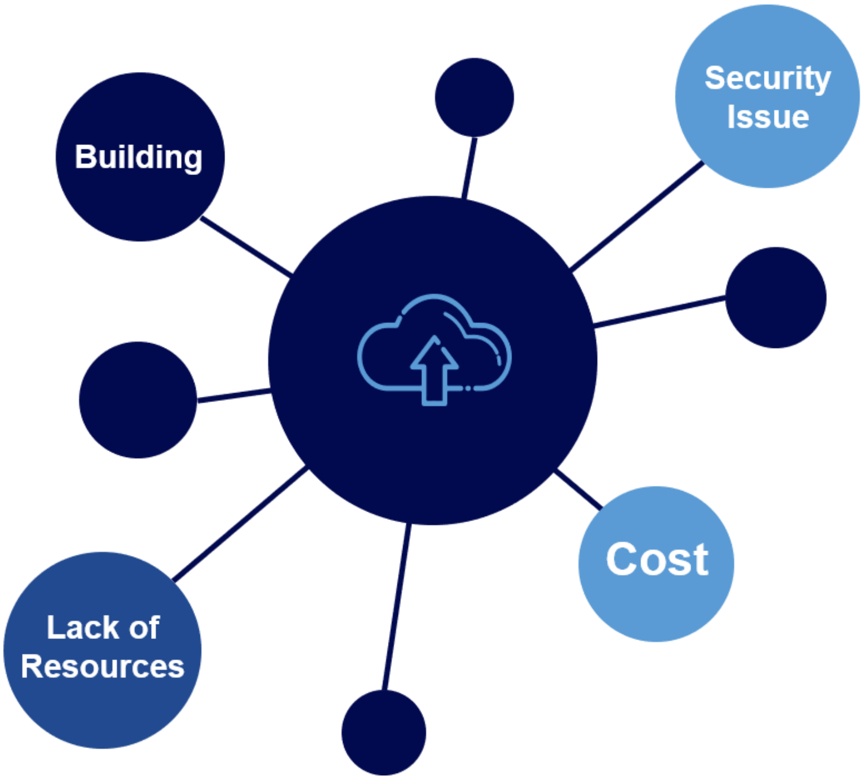

Figure 3: Cloud Security Challanges

To ensure a secure virtualized environment, proper management procedures, security architecture, and controls are imperative. Security failures can occur due to various factors, including hardware loss, software malware, the execution of harmful programs by clients, application breakdowns, or unauthorized access to client applications by third parties, resulting in the introduction of incorrect data.(Abdelrahman *et al.*, 2021)

II. Cloud Computing- Historical Perspective:

Computing in the cloud is one of the internet service models that is expanding at the quickest rate. The Institute of Standards and Technology (NIST) defines the computing such as “system that depends on four different deployment techniques”. It integrates both software and hardware in order to provide consumers with a variety of processing services that can be accessed over the internet. Large-scale internet server infrastructures that are accessible by several users at the same time are created by cloud service providers. (Telo, no date)This indicates that they provide on-demand computing capabilities like as high-performance processing and memory without making the customer provide any specialised gear of their own. The concept of "cloud computing" originates from the cloud icon, which is often shown in schematics to symbolise the internet. (Sunyaev, 2020) Users may have different preferences, but adopting cloud-based systems often involves making adjustments to existing frameworks. It's worth noting that security breaches in cloud services are relatively rare. The security of your current system directly influences how secure you perceive cloud computing to be. Systems managed by expert cloud providers are generally less prone to breaches compared to internal systems managed by a team with various responsibilities. Using cloud-based services can significantly reduce the amount of IT resources needed for business operations, offering a flexible and scalable operating environment for users. In recent years, cloud computing has established itself as an integral part of the Internet's service models with the fastest rising growth rate. Institute of Standards and Technology (NIST), elaborates that idea of cloud computing is based on four primary deployment methodologies, three unique service models, and four essential characteristics. (Wani, Rana and Pandey, 2019) This comprehensive framework forms the backbone of the cloud computing infrastructure, illustrating the versatility and complexity inherent in the cloud-based service paradigm.

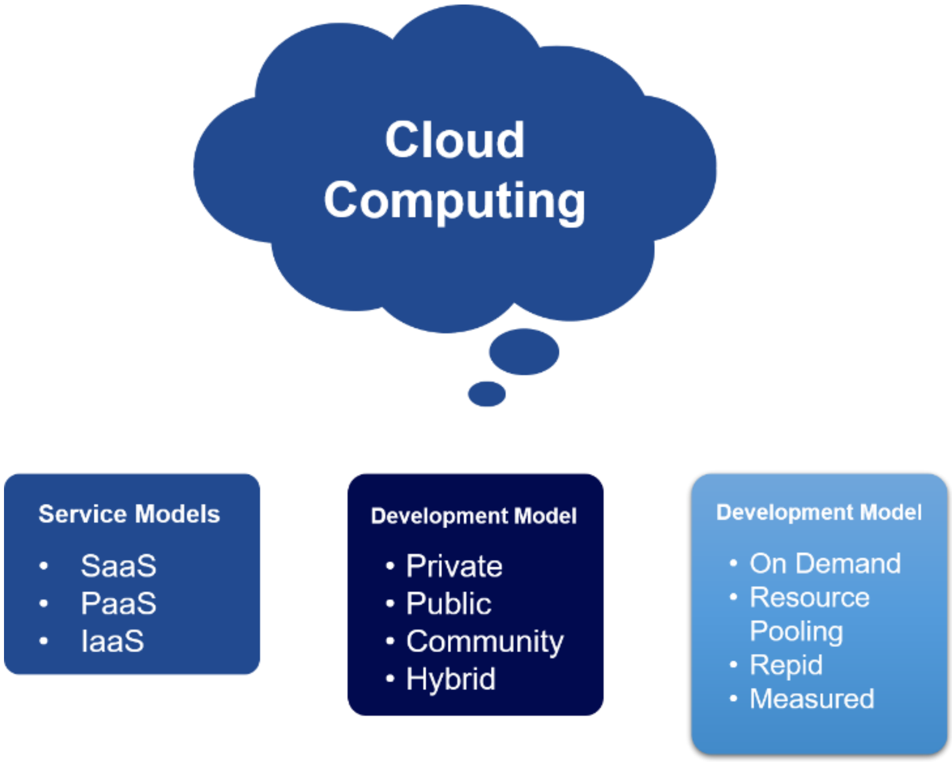

Figure 4 : Cloud Computing Models

The following list of crucial qualities that distinguish cloud computing from conventional computing includes:(Zhang, 2020)

• *On-Demand Self-Service:* In computing in the cloud, information technology resources are made available automatically on needed basis lacking direct human contact by every single service provider. This eliminates the need for personnel to monitor and manage resource allocation. This includes provisions such as network storage or server time, which are readily accessible without the need for manual intervention.

• *Vast Network Access:* Cloud resources are made available through standard network protocols and various thick or thin clients. These clients can range from traditional laptop PCs to modern devices like tablets and mobile phones, ensuring that cloud services can be accessed seamlessly via the network.(Sasubilli and R, 2021)

• *Resource Pooling*: Cloud service providers employ a dynamic approach that combines their computing capabilities with a variety of virtual and physical resources. These resources include storage, processing power, memory, internet bandwidth, and virtual machines, which are shared among multiple customers using a multi-tenant model.

• *Rapid Elasticity:* Cloud computing offers a swift and elastic capability for scaling up or down, often providing seemingly limitless capacity that can be acquired on-demand. This flexibility allows for quick adjustments to meet varying workload demands without significant delays or disruptions.

• *Measured Service:* Cloud service providers autonomously monitor, track, and optimise the utilisation of a given level of resources at a certain degree of abstraction. This approach to measured services promotes openness among the organisation that provides and the consumer, which helps to ensure that the products and services are consistently tracked and priced correctly and that they are optimised for efficiency.(Youssef, 2019)

Service Models

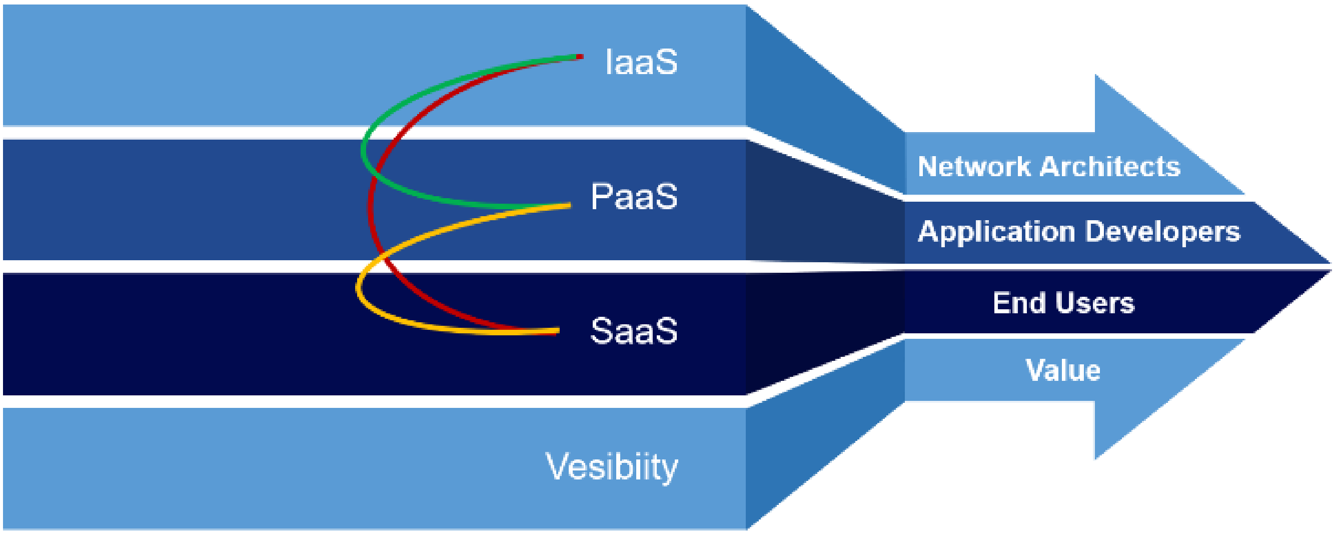

Figure 4 : Cloud obtains all necessary cloud resources in the form of services.

Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS)— are three widely-known service models, which are utilized to propose cloud computing services. (Qureshi *et al.*, 2021)

SOFTWARE AS A SERVICE (SAAS): Software as a Service, often called SaaS, is a kind of cloud computing in which customers have access to the applications of a corporation via the usage of the internet. This indicates that you are not required to download and install the programme on your computer in order to use it; rather, you may use it immediately from inside your web browser application. The firm that is delivering the software is the one that is responsible for everything that occurs in the background, including the storage of your data and the maintenance of the program's functionality. the Salesforce.com platform and Oracle Customer Relationship Management are both widely recognised instances of software as a service (SaaS) companies that provide a variety of commercially available applications that can be accessed through the internet.(El Makkaoui *et al.*, 2016)

PLATFORM AS A SERVICE (PAAS): With Platform as a Service (PaaS), a client is able to design and operate their own apps on cloud infrastructure by making use of the instruments and languages for programming that are offered by the application's service provider. Even if the client has some say over the settings of the software's configuration and the computer's hosting surroundings, they are silent about cloud infrastructure to the effect of hosting of application. Google Applications Platform and Force.com, which are two examples of cloud computing services that fall under the PaaS umbrella.

INFRASTRUCTURE AS A SERVICE (IAAS): When it comes to infrastructure as a service (IaaS), end user has an ability to install programmes using a variety of computer resources, such as networks, computing capacity, and storage space. These applications may include a variety of software and operating systems. Operating systems, computer storage, and software application deployment are all within the client's control; but, the customer does not have control over the computer network infrastructure itself. IaaS providers include the popular Amazon Web Services, the company's Azure, and Google's Compute Engine subsidiary (GCE), all of which give access to computing resources in virtualization through the internet. A few additional instances of IaaS suppliers are Rackspace and IBM Cloud.(Tahirkheli *et al.*, 2021)

Additionally, cloud computing offers four fundamental models for service delivery: cloud

computing may be broken down into four categories: the publicly accessible cloud, the privately owned cloud, the community-oriented cloud, and the cloud that is hybrid. These models are applicable to all types of services (IaaS, PaaS, or SaaS).

Development Models

The generally available the cloud, the one for individuals, the hybrid cloud, and the community-based community cloud constitute the final four distribution techniques for the private cloud. These different approaches each come with their own set of benefits and drawbacks.(*Comparative Analysis of Various Cloud Security Frameworks by Ashima Narang, Deepali Gupta :: SSRN*, no date) As a consequence of this, selecting a particular deployment strategy might turn out to be a big and difficult choice. It's important to carefully evaluate the distinct features and benefits of each deployment strategy to determine which one aligns best with your particular needs and requirements.(Zaman *et al.*, 2021)

Design of Clouds

The four most crucial components are the most affected by distributed computing, closely followed by its security ideas. Fig. Depicts the cloud computing architecture. The figure shows the Open Systems Interconnection Model's (OSI) reference architecture from start to finish. The cloud's technology is a complex system with several weaknesses.(El Kafhali, El Mir and Hanini, 2022a)

Table 1. Comparison of cloud deployment models

Models	Advantages	Disadvantages
Publics	High ascendible Cost-effective Reliability Location independence	Less secure Less customizability
Private	Higher reliability More control over the system Enhanced security and protection.	Limited visibility into the system Challenges in scaling operations Limited availability of certain services Higher risk of security breaches.
Community	Higher security compared to the public cloud Lower cost compared to the private cloud Greater flexibility and scalability.	Data segregation for enhanced privacy and security. Responsibilities are distributed within the organization for effective management.
Hybrid	High scalability for handling varying workloads efficiently. Cost-effectiveness compared to some other deployment models. Greater flexibility to adapt to changing business needs.	Ensuring security compliance can be complex. Dependence on specific infrastructure may limit flexibility.

- *Cloud Consumer:* A person or a business that uses services based on the cloud while continuing their work and communication.
- *Cloud Provider:* A provider, whether it be a person, a company, or both, who makes their products and services available to third parties through the internet.
- *Cloud Auditor:* A neutral third party that performs an analysis of cloud clients' relationships, system of information activities, achievement, and the security precautions of cloud users.
- *Cloud Broker:* An organisation that is responsible for the use, deployment, and transfer of different services delivered via cloud and acts as a mediator between cloud consumers and providers of cloud services.
- *Cloud Carrier:* A platform that makes the process of migrating to the cloud easier by facilitating the movement and transfer of services delivered via cloud from companies offering cloud services to cloud computing consumers.(*Security framework for cloud based electronic health record (EHR) system | Semantic Scholar*, no date)

III. Categorization of Cloud Threats

Even though it has its own unique set of security issues, shared computing is a solution that is quickly gaining popularity and has a great deal of untapped promise. Considering the principles of the CIA Triad (Confidentiality, Integrity, and Availability) and the potential attacks on various components of the cloud, we need to address certain issues. (Telo, no date)

CIA Cloud Security Threats

When it comes to security threats in cloud computing, they are mainly categorized under concerns related to the confidentiality, integrity, and availability of data.(El Kafhali, El Mir and Hanini, 2022b)

CONFIDENTIALITY THREATS

Concerns about data security, the possibility of being attacked from the outside, and compromises of customer information that occur on the inside are all examples of potential dangers to confidentiality.

Cloud apps that run in a welcoming atmosphere are especially vulnerable to the danger of being attacked from the outside. Attacks against cloud users and apps might occur as a result of global hardware, software, or both vulnerabilities if this danger materialises. Another significant risk is data leakage, where the sensitive information handled by clouds might be compromised due to a failure in secure access, potentially leading to serious consequences.(*Electronics | Free Full-Text | Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions*, no date)

INTEGRITY THREATS

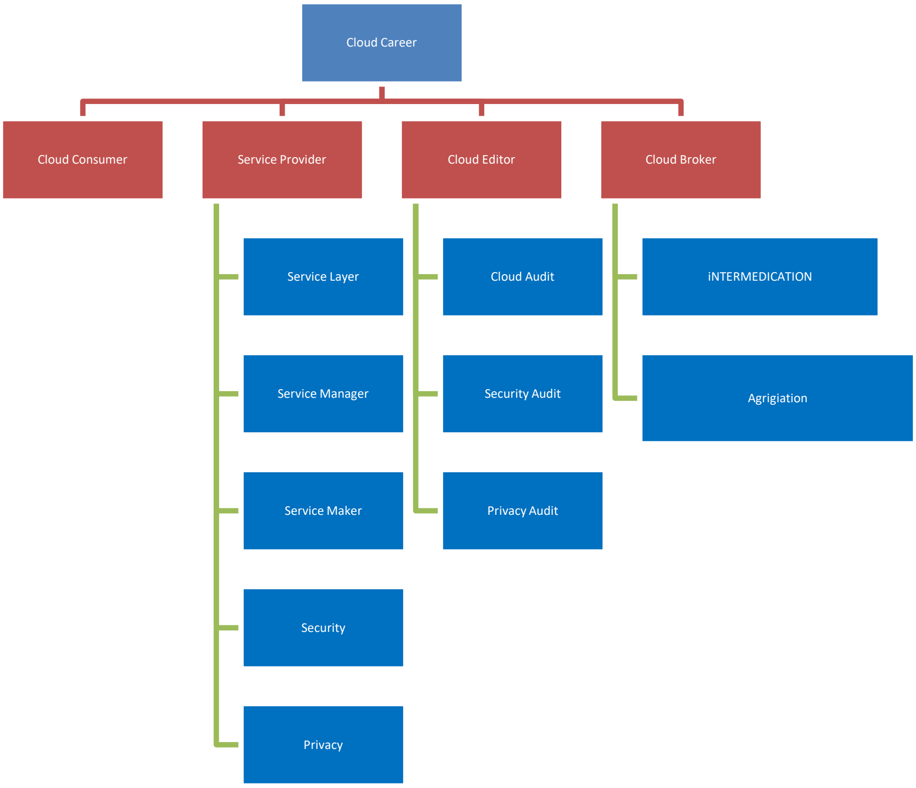

Figure 5 : Cloud Computing Architecture

Integrity threats in cloud computing encompass risks related to data separation, weak customer access management, and data quality. Data separation risks arise from incorrect implementation of secure boundaries, imprudent Virtual Machine configurations, and hypervisors based on the customer's side. These risks may be more tough to manage in a cloud setting since the cloud infrastructure allots capabilities to customers, and any change in these resources might put the dependability of the data at risk. Poor customer authentication and authorization soon follows, eventually resulting in a variety of challenges and vulnerabilities as a result of breached entry and identification control, which ultimately provides possibilities for hackers to modify information storage devices.(*Cloud Security Threats and Solutions: A Survey | Wireless Personal Communications*, no date)

AVAILABILITY THREATS

Furthermore, availability threats highlight the impact of governance on progress, lack of connectivity, genuine interference with resources, and ineffective recovery procedures. The impact of governance on progress refers to the challenges stemming from client access testing for different users and institutional modifications. Changes within the cloud environment, its content, and applications can adversely affect the accessibility of cloud services. Non-availability of services is another concern, encompassing the unavailability of network bandwidth, DNS affiliation registration issues, and resource scarcity. Additionally, genuine interference with IT departments of service providers, cloud consumers, and WAN service providers can significantly disrupt operations. Lastly, inefficient recovery processes, such as inadequate failure recovery, can impact the duration and effectiveness of the recovery process in the event of an incident.(Swathy Akshaya and Padmavathi, 2019)

Comparative Analysis of Attacks on the Bases of Cloud Components

In order to provide a comparative analysis, attacks in the context of cloud computing are categorized based on their components. This categorization allows for a more comprehensive understanding of the various types of threats and vulnerabilities that may arise within each specific component of the cloud infrastructure.(Tabrizchi and Kuchaki Rafsanjani, 2020)

NETWORK-TARGETED ATTACKS

This article examines three different types of frame threats: network checking attacks, botnet attacks, and spoofing attacks. Scanning ports may be useful for hackers since it enables them to get relevant information that can be used to carry out an attack successfully. Defenders often do not disguise their identities when undergoing port inspections, in contrast, attackers frequently do so. This is true even if a company's security surveillance staff routinely examines the ports. A botnet is a network of personal computers, cell phones, or other internet-connected devices that have been infected with malware and may be remotely manipulated by malicious cybercriminals. When working in concert, these compromised gadgets open the door to a wide range of potentially harmful acts. (Nhlabatsi *et al.*, 2021)

Attacks known as spoofing occur when a computer technician or a different malicious player pretends to be information dishonestly with the purpose of giving a technological advantage to a different user. This occurs when a third party from outside the organisation poses as another entity, like as a machine or a phone, inside the organisation in order to coerce other devices, gadgets, or persons into performing certain activities or disclosing sensitive information. For example, this may be a phone or a computing device.(*Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal | Journal of Reliable Intelligent Environments*, no date)

VIRTUAL MACHINE-CENTRIC ATTACKS

The presence of numerous virtual machines within a system can potentially lead to various security risks. These risks can include the exploitation of performance data on the system, which is unrelated to any faults in the code, resulting in what is known as a side-channel attack. This type of attack is capable of extracting sensitive information from a system by analyzing its patterns and operations, even if there are no direct vulnerabilities in the system's software. When a malware code is implanted within the VM-image, it can be duplicated during the creation process of new virtual machines. It's crucial for the system's administrators to thoroughly examine and analyze the virtual machine image's configuration and content. By implementing effective sorting and filtering mechanisms, administrators can proactively identify, address, and recover from potential security threats that may arise within the virtual machine environment.

DATA REPOSITORY ATTACKS

When a comprehensive monitoring system isn't in place, attackers can sneakily get hold of important information stored on specific devices. Information skimming means taking out data from a storage source without actually erasing it, giving attackers a way to get or use it for their own purposes. "Information de-duplication" is when data that's already there gets copied. To deal with this type of attack, it's important to have safeguards in place that ensure copying only happens when we need to figure out how many identical records there are. Cloud computing has gained huge attention over the past decades because of continuously increasing demands. (*Comparison of Cloud Computing Security Threats and Their Counter Measures | SpringerLink*, no date). There are several advantages to organizations moving toward cloud-based data storage solutions. These include simplified IT infrastructure and management, remote access from effectively anywhere in the world with a stable Internet connection and the cost efficiencies that cloud computing can bring. The associated security and privacy challenges in cloud require further exploration. Researchers from academia, industry, and standards organizations have provided potential solutions to these challenges in the previously published studies. The narrative review presented in this survey provides cloud security issues and requirements, identified threats, and known vulnerabilities. In fact, this work aims to analyze the different components of cloud computing as well as present security and privacy problems that these systems face. Moreover, this work presents new classification of recent security solutions that exist in this area. Additionally, this survey introduced various types of security threats which are threatening cloud computing services and also discussed open issues and propose future directions. This paper will focus and explore a detailed knowledge about the security challenges that are faced by cloud entities such as cloud service provider, the data owner, and cloud user.(Sureshkumar and Baranidharan, 2021)

SOFTWARE-CENTRIC ATTACKS

An application running in the cloud can face a range of threats, one of the most significant being the risk of data seepage for malicious drives. The three crucial assaults that target cloud-based applications include:

Malware Insertion and Cryptographic Attacks: These involve the introduction of harmful software or exploitation of weaknesses in the application's encryption systems, potentially leading to unauthorized access and data breaches.(Jouini and Rabai, 2019)

Shared Schemes, Web Services, and Display-Based Attacks: These attacks are aimed at compromising the security of shared data schemes, web services, or the visual aspects of the application. They can result in unauthorized access, data tampering, or other security breaches, potentially exposing sensitive information to unauthorized parties.(*A security evaluation framework for cloud security auditing | The Journal of Supercomputing*, no date)

IV. Cloud Computing-Vulnerabilities

Here we will discuss the major risks acknowledged to be linked with the use of cloud computing. The following are some of these dangers:

Dangers to information, include breaches of confidentiality and informational material loss. Risks to networks include unauthorized access to accounts or services as well as attacks that result in a denial of service. Threats that are unique to the cloud environment include insecure communication channels and APIs, threats from insiders, improper usage of cloud services, a lack of proper precautionary measures, and weaknesses in collaborative software development.(Kumar and Goyal, 2019)

Data Intimidations

The protection of data is becoming more important as an increasing number of users move their files to the cloud. Data is seen as an essential asset for every business. The data production stage, the processing stage, the storage stage, the deletion stage, and the transition stage are all part of the information's complete life cycle that occurs in the cloud. It is possible for data to be produced on an internet-connected clients or server, then transmitted into the online environment via a system, and finally temporarily stored there. It is the responsibility of the provider of services to guarantee that the platform is safe and fitted with the appropriate security measures in order to keep the data from being compromised, which is a tough challenge in and of itself.(Kumar and Goyal, 2019)

DATA BREACHES

Data breaches involve the leakage of sensitive customer or any data related to an organization without any authority. Such incidents can harm any company in terms of finances and customer's trust. Data breaches often occur due to vulnerabilities in infrastructure, application design, inadequate authentication, and oversight controls.(*A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies | IEEE Journals & Magazine | IEEE Xplore*, no date)

DATA LOSS

Data loss is a vital concern within cloud security, which can result from various factors such as partial file disconnection, access to delicate data without any authority, or the damage of encryption keys. Like data breaches, data loss can harm an organization, and it can be caused by malicious attacks, data deletion, loss of encryption keys, system failures, or natural disasters. Cloud applications have also been targeted by malware attacks, leading to data destruction.

ADVANCED PERSISTENT THREATS

Advanced Persistent Threats (APTs) refer to attacks where unauthorized individuals gain long-term access to a system or network without being detected. APTs pose a significant risk to businesses, as attackers with continuous access to sensitive data can create serious vulnerabilities for organizations.

V. Methods Related to Cloud Security

Counter-measures for Security Jeopardies

Organizations that share resources face data misuse concerns, hence the critical need for robust data security measures to prevent data loss and its negative impacts on businesses and trust within organizations.(Gudapati Syam Prasad and S. Gaikwad, 2018)

REMEDIES FOR DATA BREACHES AND SYSTEM VULNERABILITIES

Implementing powerful security arrangements is the most effective defense to tackle such data breaches. Using multifactor authentication (MFA) encryption are vital security methods that can significantly enhance cloud security. Best practices include regular vulnerability scans and prompt addressing of identified device threats.

COUNTERMEASURES FOR CREDENTIAL AND ACCESS MANAGEMENT

For both cloud service users and operators, the implementation of multifactor authentication mechanisms, such as smart cards, one-time passwords (OTP), and mobile authentication, is essential. These mechanisms make it significantly more challenging for hackers to gain unauthorized access through compromised passwords, thereby enhancing the overall security posture.(*Cloud Computing—Security, Issues, and Solutions | SpringerLink*, no date)

COUNTERMEASURES FOR INSECURE INTERFACES AND APIS.

To review Security code means examining the source code of an application to ensure the presence of enough security authorizations which function as intended and are entreated in a number of instances. Penetration testing is also beneficial in determining a system's vulnerability to potential attacks, identifying any existing weaknesses, and overcoming any successful resistance during the testing process.

ACCOUNT HIJACKING AND SERVICE DENIAL-COUNTERMEASURES:

Organizations should proactively identify these threats and engage quality d security practices to remove potential damages including legal repercussions resulting from security breaches. Preventing the sharing of account credentials among users and services, adopting two-factor authentication, and investing in substantial bandwidth are effective strategies in countering hijacking and denial of service attacks. Additionally, regularly updated detection protocols play a significant role in defending against sophisticated cyberattacks targeting companies and government organizations, especially those that necessitate interaction/action by the user.(Swathy Akshaya and Padmavathi, 2019)

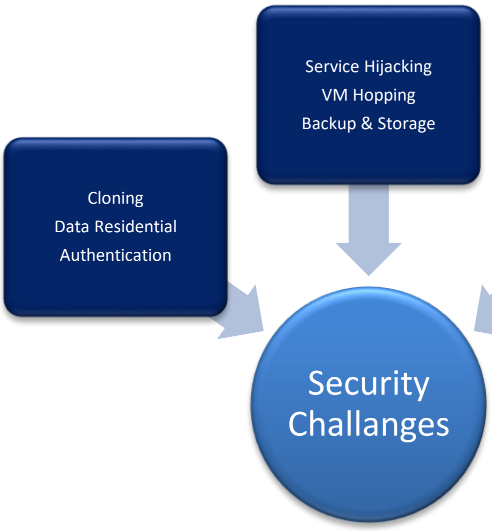

Figure 6 : Cloud Computing Security Challanges

VI. Trusted Cloud Computing & Cloud Execution Environment:

Trusted cloud computing is used to ensure data security, integrity, and efficient computations. To achieve this, various measures are implemented, such as:

Implementation of Field-Programmable Gate Arrays (FPGAs) for secure and protected identification of calculations within the logic fabric. FPGAs store systematic and symmetric encryption in their memory, ensuring secure application processing on cloud servers. Use of Distributed Hash Tables (DHTs) to enhance cloud security, preventing intrusions and Distributed Denial of Service (DDoS) attacks. Application of data coloring-based watermarking to protect data objects within the cloud environment, with different colors and properties indicating various security levels known only to the owners. Trust integrators play a role in maintaining trust and also in negotiating parameters. Application of watermarking techniques to secure the runtime environment of cloud systems, protecting Java programs with specific watermark algorithms and executing only those programs with matching watermarks. Unmatched programs trigger error messages and unauthorized execution prevention. Implementation of symmetric and asymmetric encryption for data confidentiality, orchestrated by a trust-worthy third party relying upon specific properties. Use of IPSEC and SSL communication mechanisms for secure communication and event protection between components, as well as the application of (SSO) and (LDAP) by digital authorization signatures. Establishment of security domains for federated clouds, facilitating cloud communication through standardized interfaces. These measures collectively contribute to a more secure cloud computing environment, ensuring the protection, integrity, and confidentiality of data and communication between various components and entities.(Aoudni *et al.*, 2022)

VII. Addressing Cloud Security and Compliance Regulations

The paper focuses on the challenges related to security and compliance in cloud computing. It delves into various issues and complexities that can arise within cloud environments, discussing their potential implications and the measures required to ensure security and regulatory compliance.

VIII. Strategies and Protective Measures against Attacks

To prevent and track computer attacks, several active defense techniques have been developed. These techniques aim to assess the attacker's actions and identify breaches early. In this section, the article focuses on DDoS (Distributed Denial of Service) attacks, particularly the countermeasures and mitigation strategies for dealing with them.(El Kafhali, El Mir and Hanini, 2022a)

Deployment of DDoS Defense

DDoS protection can be employed at 4 critical points namely the source end, the access point, the intermediate network, and the distributed network. Source-End Deployment: This approach focuses on securing network resources and bandwidth. It often involves using throttling tools to slow down the speed of packets during a potential DDoS attack.(Potluri *et al.*, 2020)

Access Point Distribution: Different levels of access points, including front-end, back-end, and virtual access points, are deployed in the cloud computing environment. DDoS protections at the access point help distinguish between legitimate and malicious traffic before granting access to cloud resources and services.

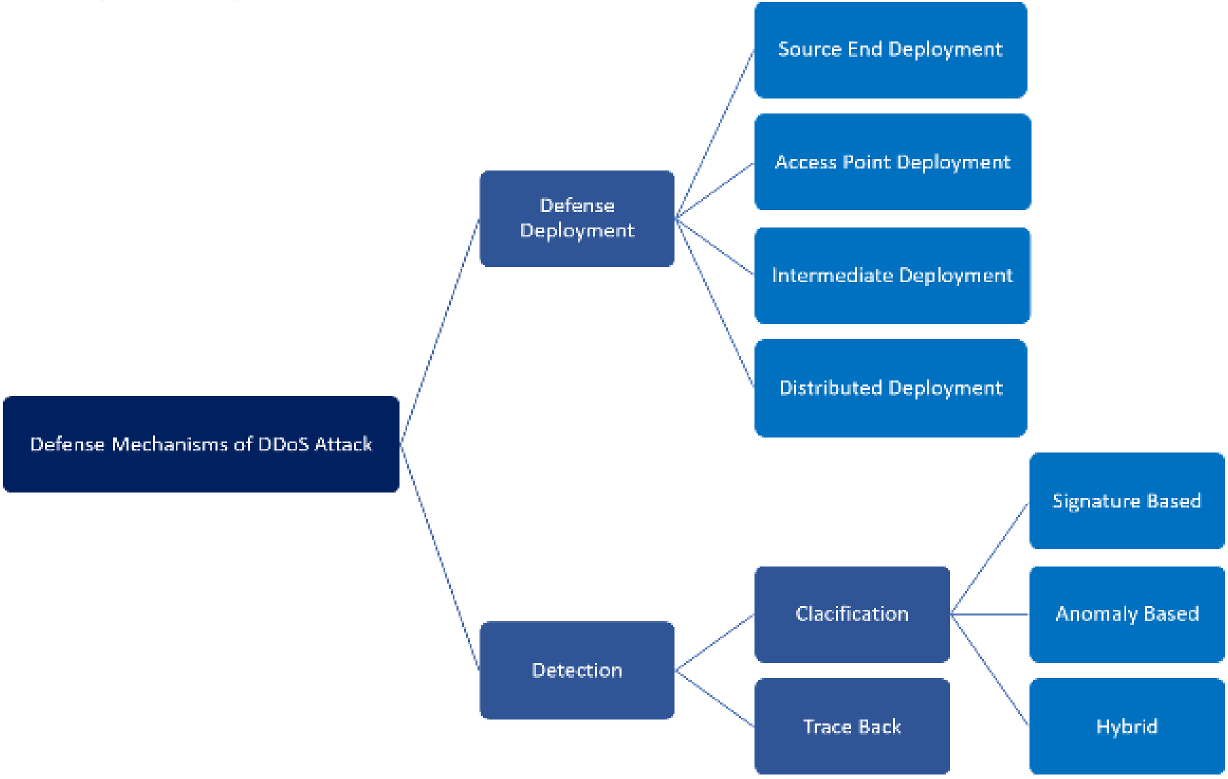

Figure 7 : DDoS Attacks & Defense Mechanisums

Intermediate-Network Deployment: Protections beingeffectuated on network nodes to lessen the effect caused by DDoS attacks before they reach the target. Rate limits may be imposed on traffic routed through each node based on a standard profile pattern.(Arif *et al.*, 2024)

Distributed Defense: This deployment framework integrates source-end, access point, and intermediate network deployment, aiming for a high detection rate of DDoS attacks.

Detection of DDoS

DDoS detection systems can be classified into three categories: signature-based, anomaly-based, and hybrid, depending on status of traffic in terms of normality. (Potluri *et al.*, 2020)

Signature-Based Detection: This method uses a set of predefined attack patterns stored in a database to identify malicious traffic. However, it can struggle to detect unknown and zero-day threats, leading to a significant number of false negatives.

Anomaly-Based Detection: Anomaly-based detection involves tracking behavioral patterns over a specific period to identify unusual network and computer activities. It distinguishes between regular and malicious activities based on predetermined heuristics or rules.(Abdullayeva, 2021)

The hybrid-based detection strategy combines elements of signature-based and anomaly-based detection methods to improve the overall detection rate while reducing false positives. Researchers have proposed adaptive decentralized Intrusion Detection Systems (IDS) that leverage irregularity-based & knowledge-based modus operandi to effectively detect and lessen DDoS attacks. These systems facilitate communication between different agents to assess false alarms and malicious nodes. To address the issue of fabricated IP addresses in DDoS attacks, trace back techniques have been suggested to trace the source of the attacks. Additionally, security measures such as the SOA-Based Trace back method and cloud filters positioned at routers help identify and bifurcate packets with faked IP addresses.(Jabir *et al.*, 2016)

In terms of intrusion avoidance, deploying Intrusion Prevention Systems (IPS) at multiple access points is recommended to prevent DDoS attacks from causing significant damage. Dynamic resource allocation mechanisms based on attacking potency are designed to improvise the Worth of Service (QoS) for genuine users. Furthermore, a hybrid Cloud-Based Firewalling architecture, incorporating both virtual and physical components, is proposed to enhance decision management and optimize overall performance. This architecture involves the analysis of incoming traffic by the Security-as-a-Service (SaaS) structure, with virtual firewalls implemented by virtual machines (VMs) playing a key role in monitoring, analyzing, and reporting on potential threats.(Abdullayeva, 2021)

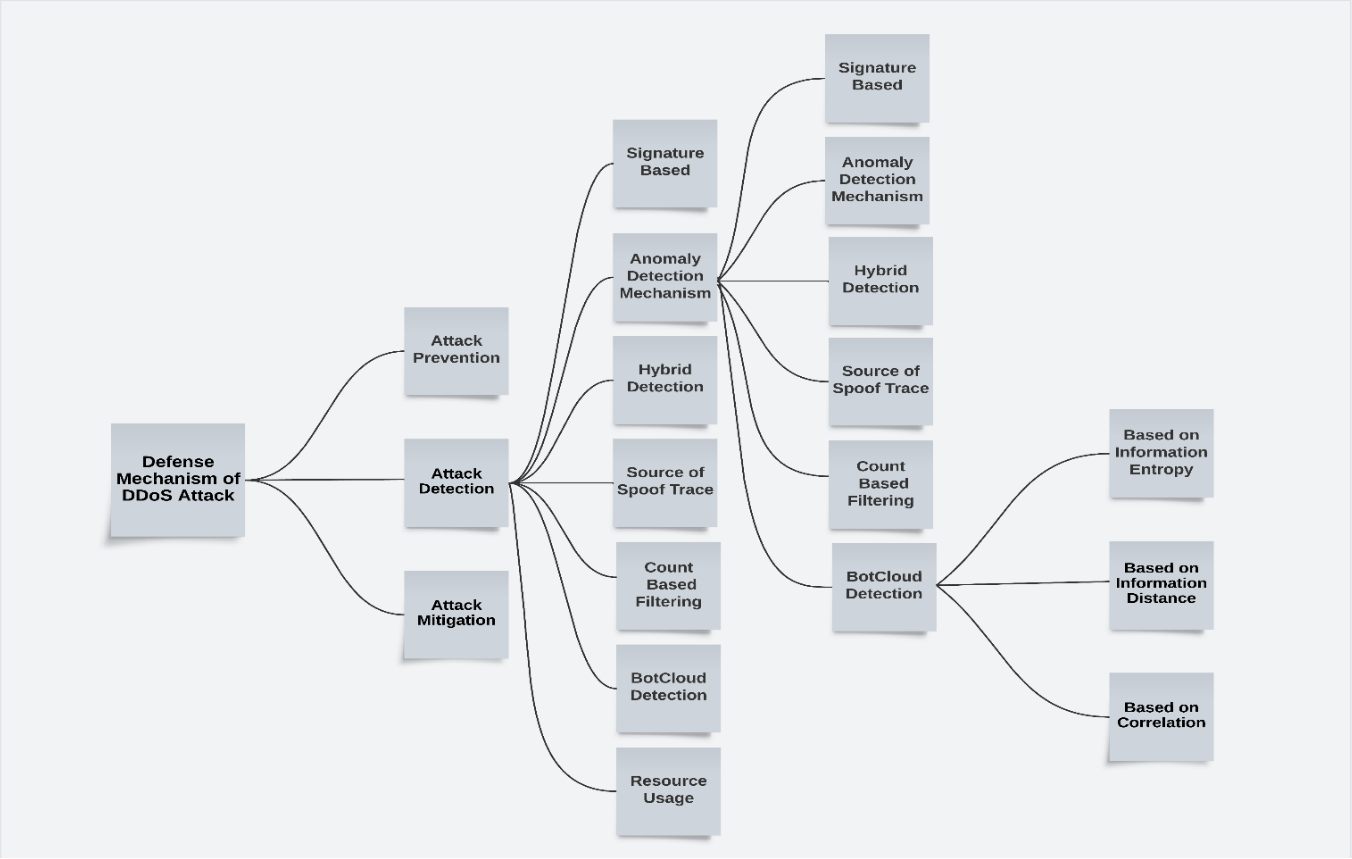

Figure 8. Methods for Defending Against DDoS assaults in Cloud Computing

Ingress blocking is a method used to configure a router by discarding incoming traffic originating from malevolent source addresses. This process involves dropping any traffic with an IP address that does not match the domain prefix associated with the ingress router. On the other hand, egress filtering is a technique that ensures only the IP address space previously assigned to the network can leave it. Egress filtering, also referred to as outward filtering, serves as a protective measure against potential threats to domains. Both ingress and egress filters operate in the same manner regardless of their placement within the network architecture. Jia et al. have proposed a poignant target security methodology, specifically the shuffling modus operandi, aimed at combating Distributed Denial of Service (DDoS) attacks in the internet environment. This technique involves replicating the vulnerable server and transferring the intelligent client to create mobile targets, thereby enabling the extraction and separate classification of the DDoS attack. This approach is designed to enhance the security of servers by making them more elusive and difficult for attackers to target.(Balboni, 2011)

IX. Ongoing Dilemmas and Future Prospects

This discuss various challenges and open problems in the field of cloud security and the emerging concept of the Cloud of Things (CoT), which is an integration of IoT devices with cloud computing. Let me explain it in simpler terms.

Cloud security is an important issue that has not been completely resolved. There are concerns about ensuring that clients have full control over their data and who can access it. Researchers have focused on different security issues, but there is a need for a more unified and comprehensive security solution for cloud computing. One important aspect is ensuring that only authorized users have access to data and that the privacy of the users is protected.(Mthunzi *et al.*, 2020)

Multi-tenancy, where multiple clients share the same resources in a cloud environment, can lead to underutilization of resources and vulnerability to DDoS attacks. Managing multiple user accounts efficiently is a major challenge in cloud security.

With the increasing number of connected devices due to the Internet of Things (IoT), there is a massive amount of data that needs to be processed and stored. Cloud computing is seen as a solution to handle the needs of IoT. However, integrating IoT with the cloud poses challenges related to data security, accessibility, and performance.

The Cloud of Things (CoT) is a new concept that facilitates the connection of IoT devices to the cloud. It offers numerous possibilities for both users and service providers, but it also comes with challenges such as reactive architecture, latency, and data processing speed.(Birje *et al.*, 2015)

Detecting authorized and malicious users in the cloud infrastructure is another significant challenge. While various technologies like artificial intelligence and machine learning are used for this purpose, integrating these technologies effectively remains a challenge. The emphasizes the need for a more comprehensive approach to cloud security, addressing issues related to data control, multi-tenancy, IoT integration, and user authentication. Resolving these challenges is crucial for ensuring the safety and efficiency of cloud computing systems in the future.

X. Conclusion

In this study, we focused on addressing the security concerns associated with cloud computing. Initially, we threw light on fundamental aspects of cloud computing, including how services are delivered, different deployment strategies, data center virtualization, and the migration of virtual machines. We also highlighted the reasons why cloud computing is favored, along with the obstacles preventing its widespread adoption. Subsequently, we delved into a diversity of security and privacy drawbacks in cloud computing, identifying the key risks and vulnerabilities and categorizing them for better understanding.

We emphasized that security and privacy are the crucial hurdles that should be addressed to establish a dependable and trustworthy computing environment. Additionally, we presented the different research directions that are currently addressing the various security concerns in cloud computing. Despite its numerous advantages, cloud computing, as a relatively new computing paradigm, poses several security challenges. Cloud deployment methods, most of them are suitable for every service, client, or interested party, as comprehensive security measures may not be feasible for all cloud companies to implement uniformly.

Cloud computing is an exciting and rapidly expanding trend in the field of information technology, significantly contributing to advancements in various applied sciences, particularly security measures. Our study extensively covered the strategies and diverse approaches to dealing with cloud computing and its associated security concerns. We aimed to bridge the gaps left by previous surveys, which often lacked in-depth analysis of the risks associated with cloud computing. Through our comprehensive examination of these security risks and the corresponding strategies and solutions, we aimed to contribute to a more comprehensive understanding of the field and provide effective measures to address the security challenges of cloud computing.

References

[1] A security evaluation framework for cloud security auditing | The Journal of Supercomputing (no date). Available at: https://link.springer.com/article/10.1007/s11227-017-2055-1 (Accessed: 10 July 2024).

[2] A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies | IEEE Journals & Magazine | IEEE Xplore (no date). Available at: https://ieeexplore.ieee.org/abstract/document/9404177 (Accessed: 10 July 2024).

[3] Abdullayeva, F.J. (2021) 'Advanced Persistent Threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm', Array, 10, p. 100067. Available at: https://doi.org/10.1016/j.array.2021.100067.

[4] Anjana and Singh, A. (2019) 'Security concerns and countermeasures in cloud computing: a qualitative analysis', International Journal of Information Technology, 11(4), pp. 683–690. Available at: https://doi.org/10.1007/s41870-018-0108-1.

[5] Aoudni, Y. et al. (2022) 'Cloud security based attack detection using transductive learning integrated with Hidden Markov Model', Pattern Recognition Letters, 157, pp. 16–26. Available at: https://doi.org/10.1016/j.patrec.2022.02.012.

[6] Arif, H. et al. (2024) 'Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research', International Journal of Multidisciplinary Sciences and Arts, 3(1), pp. 242–251. Available at: https://doi.org/10.47709/ijmdsa.v2i2.3452.

[7] Balboni, P. (2011) 'Data Protection and Data Security Issues Related to Cloud Computing in the EU', in N. Pohlmann, H. Reimer, and W. Schneider (eds) ISSE 2010 Securing Electronic Business Processes. Wiesbaden: Vieweg+Teubner, pp. 163–172. Available at: https://doi.org/10.1007/978-3-8348-9788-6_16.

[8] Birje, M. et al. (2015) 'Security Issues and Countermeasures in Cloud Computing', International Journal of Applied Engineering Research, 10, pp. 71–75.

[9] Cloud Computing—Security, Issues, and Solutions | SpringerLink (no date). Available at: https://link.springer.com/chapter/10.1007/978-981-15-5397-4_70 (Accessed: 10 July 2024).

[10] Cloud Security Threats and Solutions: A Survey | Wireless Personal Communications (no date). Available at: https://link.springer.com/article/10.1007/s11277-022-09960-z (Accessed: 13 July 2024).

[11] Comparative Analysis of Various Cloud Security Frameworks by Ashima Narang, Deepali Gupta :: SSRN (no date). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329394 (Accessed: 10 July 2024).

[12] Comparison of Cloud Computing Security Threats and Their Counter Measures | SpringerLink (no date). Available at: https://link.springer.com/chapter/10.1007/978-3-030-43192-1_25 (Accessed: 13 July 2024).

[13] Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal | Journal of Reliable Intelligent Environments (no date). Available at: https://link.springer.com/article/10.1007/s40860-020-00115-0 (Accessed: 10 July 2024).

[14] Discover the Cloud Security Threats in 2018 - Cisco Community (no date). Available at: https://community.cisco.com/t5/security-blogs/discover-the-cloud-security-threats-in-

2018/ba-p/3664430 (Accessed: 12 October 2023).

[15] El Kafhali, S., El Mir, I. and Hanini, M. (2022a) 'Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing', Archives of Computational Methods in Engineering, 29(1), pp. 223–246. Available at: https://doi.org/10.1007/s11831-021-09573-y.

[16] El Kafhali, S., El Mir, I. and Hanini, M. (2022b) 'Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing', Archives of Computational Methods in Engineering, 29(1), pp. 223–246. Available at: https://doi.org/10.1007/s11831-021-09573-y.

[17] El Makkaoui, K. et al. (2016) 'Cloud security and privacy model for providing secure cloud services', in 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech). 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), pp. 81–86. Available at: https://doi.org/10.1109/CloudTech.2016.7847682.

[18] Electronics | Free Full-Text | Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions (no date). Available at: https://www.mdpi.com/2079-9292/11/20/3330 (Accessed: 10 July 2024).

[19] Gudapati Syam Prasad, D. and S. Gaikwad, V. (2018) 'A Survey on User Awareness of Cloud Security', International Journal of Engineering & Technology, 7(2.32), p. 131. Available at: https://doi.org/10.14419/ijet.v7i2.32.15386.

[20] Internet of Things: Security Vulnerabilities and Countermeasures - IOPscience (no date). Available at: https://iopscience.iop.org/article/10.1149/10701.15043ecst/meta (Accessed: 10 July 2024).

[21] Jabir, R.M. et al. (2016) 'Analysis of cloud computing attacks and countermeasures', in 2016 18th International Conference on Advanced Communication Technology (ICACT). 2016 18th International Conference on Advanced Communication Technology (ICACT), pp. 117–123. Available at: https://doi.org/10.1109/ICACT.2016.7423296.

[22] Jouini, M. and Rabai, L.B.A. (2019) 'A Security Framework for Secure Cloud Computing Environments', in Cloud Security: Concepts, Methodologies, Tools, and Applications. IGI Global, pp. 249–263. Available at: https://doi.org/10.4018/978-1-5225-8176-5.ch011.

[23] Khoda Parast, F. et al. (2022) 'Cloud computing security: A survey of service-based models', Computers & Security, 114, p. 102580. Available at: https://doi.org/10.1016/j.cose.2021.102580.

[24] Kumar, R. and Goyal, R. (2019) 'On cloud security requirements, threats, vulnerabilities and countermeasures: A survey', Computer Science Review, 33, pp. 1–48. Available at: https://doi.org/10.1016/j.cosrev.2019.05.002.

[25] Mthunzi, S.N. et al. (2020) 'Cloud computing security taxonomy: From an atomistic to a holistic view', Future Generation Computer Systems, 107, pp. 620–644. Available at: https://doi.org/10.1016/j.future.2019.11.013.

[26] Potluri, S. et al. (2020) 'Detection and Prevention Mechanisms for DDoS Attack in Cloud Computing Environment', in 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). 2020 11th International Conference on Computing,

Communication and Networking Technologies (ICCCNT), Kharagpur, India: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/ICCCNT49239.2020.9225396.

[27] Qureshi, K.N. et al. (2021) 'Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges With Future Aspects', IEEE Transactions on Intelligent Transportation Systems, 22(3), pp. 1777–1786. Available at: https://doi.org/10.1109/TITS.2020.2994972.

[28] Sasubilli, M.K. and R, V. (2021) 'Cloud Computing Security Challenges, Threats and Vulnerabilities', in 2021 6th International Conference on Inventive Computation Technologies (ICICT). 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India: IEEE, pp. 476–480. Available at: https://doi.org/10.1109/ICICT50816.2021.9358709.

[29] Secure Cloud Storage: A framework for Data Protection as a Service in the multi-cloud environment | IEEE Conference Publication | IEEE Xplore (no date). Available at: https://ieeexplore.ieee.org/abstract/document/7346879/ (Accessed: 10 July 2024).

[30] Security framework for cloud based electronic health record (EHR) system | Semantic Scholar (no date). Available at: https://www.semanticscholar.org/paper/Security-framework-for-cloud-based-electronic-%28EHR%29-Ganiga-Pai/2e5a9da2c0f24865b331855c4adfb80992da0f78?p2df (Accessed: 10 July 2024).

[31] Sunyaev, A. (2020) 'Cloud Computing', in Sunyaev, A., Internet Computing. Cham: Springer International Publishing, pp. 195–236. Available at: https://doi.org/10.1007/978-3-030-34957-8_7.

[32] Sureshkumar, V. and Baranidharan, B. (2021) 'A study of the cloud security attacks and threats', Journal of Physics: Conference Series, 1964(4), p. 042061. Available at: https://doi.org/10.1088/1742-6596/1964/4/042061.

[33] Swathy Akshaya, M. and Padmavathi, G. (2019) 'Taxonomy of Security Attacks and Risk Assessment of Cloud Computing', in J.D. Peter, A.H. Alavi, and B. Javadi (eds) Advances in Big Data and Cloud Computing. Singapore: Springer Singapore (Advances in Intelligent Systems and Computing), pp. 37–59. Available at: https://doi.org/10.1007/978-981-13-1882-5_4.

[34] Tabrizchi, H. and Kuchaki Rafsanjani, M. (2020) 'A survey on security challenges in cloud computing: issues, threats, and solutions', The Journal of Supercomputing, 76(12), pp. 9493–9532. Available at: https://doi.org/10.1007/s11227-020-03213-1.

[35] Tahirkheli, A.I. et al. (2021) 'A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges', Electronics, 10(15), p. 1811. Available at: https://doi.org/10.3390/electronics10151811.

[36] Telo, J. (no date) 'Smart City Security Threats and Countermeasures in the Context of Emerging Technologies'.

[37] Wani, A.R., Rana, Q.P. and Pandey, N. (2019) 'Analysis and Countermeasures for Security and Privacy Issues in Cloud Computing', in P.K. Kapur et al. (eds) System Performance and Management Analytics. Singapore: Springer Singapore (Asset Analytics), pp. 47–54. Available at: https://doi.org/10.1007/978-981-10-7323-6_4.

[38] What are the IaaS, PaaS, and SaaS Cloud Service Models? (no date). Available at:

https://qualitapps.com/en/what-are-the-iaas-paas-and-saas-cloud-service-models/ (Accessed: 12 October 2023).

[39] Youssef, A.E. (2019) 'A Framework for Cloud Security Risk Management based on the Business Objectives of Organizations', International Journal of Advanced Computer Science and Applications, 10(12). Available at: https://doi.org/10.14569/IJACSA.2019.0101226.

[40] Zaman, S. et al. (2021) 'Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey', IEEE Access, 9, pp. 94668–94690. Available at: https://doi.org/10.1109/ACCESS.2021.3089681.

[41] Zhang, R. (2020) 'The impacts of cloud computing architecture on cloud service performance', Journal of Computer Information Systems, 60(2), pp. 166–174. Available at: https://doi.org/10.1080/08874417.2018.1429957.