I.J. Information Technology and Computer Science, **2024, 4, 1-28**
Published Online on August 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2024.04.01

Securing the Cloud Infrastructure: Investigating Multi-tenancy Challenges, Modern Solutions and Future Research Opportunities

Md. Abul Hayat*
Department of Computer Science & Engineering, IMT School for Advanced Studies Lucca, Piazza S.Francesco, 19, 55100 Lucca LU, Italy
E-mail: abul.hayat@imtlucca.it
ORCID iD: https://orcid.org/0009-0001-9286-074X
*Corresponding author

Sunriz Islam
Department of Telecommunication & Electronics Engineering, Hajee Mohammad Danesh Science and Technology University, Basherhat, N508, 5200, Dinajpur, Bangladesh
E-mail: sunrizislam@gmail.com
ORCID iD: https://orcid.org/0009-0003-3443-478X

Md. Fokhray Hossain
Department of computer science & engineering, Daffodil International University, Daffodil Smart City, Birulia 1216, Dhaka, Bangladesh
E-mail: drfokhray@daffodilvarsity.edu.bd
ORCID iD: https://orcid.org/0000-0001-7076-3079

Received: 10 January 2024; Revised: 13 March 2024; Accepted: 17 May 2024; Published: 08 August 2024

Abstract: Industry heavyweights like Microsoft, Amazon, and Google are at the forefront of the development and provision of cutting-edge and affordable cloud computing solutions, contributing to the widespread recognition of cloud computing. Without requiring direct human control, this technology provides network services, including data storage and computational power. But security becomes apparent as a major issue, hindering widespread adoption. The present study performs an extensive investigation to investigate security concerns related to cloud computing at several infrastructure levels, including application, network, host, and data. It examines significant issues that could impact the business model for cloud computing and discuss ways to solve security issues at every level that have been documented in the literature. The study identifies open problems, especially when considering cloud capabilities like elasticity, flexibility, and multi-tenancy, which create new problems at every infrastructure tier. Notably, it is found that multi-tenancy has a significant influence, contributing to security issues at all levels including abuse, unavailability, data loss, and privacy violations. The research ends with practical recommendations for additional studies targeted at improving overall cloud computing security. The results highlight the necessity of concentrated effort on mitigating security vulnerabilities resulting from multi-tenancy. This study makes a valuable contribution to the wider discussion on cloud security by identifying particular issues and supporting focused initiatives to strengthen the resilience of cloud infrastructure.

Index Terms: Cloud Computing, Cloud Security, Cloud Security Challenges, Application Security, Network Security, Data Security, Host Security.

1. Introduction

The on-demand deployment of computer resources (including storage and infrastructure) via the internet is known as cloud computing. It eliminates the need for individuals and businesses to pay for just the tangible resources they use. Systems for cloud computing are expansive, diverse groups of independent systems with adaptable computational architecture. This technology is gaining popularity since it is regarded as the greatest choice for businesses who do not

want to employ development staff or handle internal system maintenance [1]. Many organizations are creating effective cloud products and technology, including Microsoft, IBM, Sun, Amazon AWS, and many more [2]. In cloud computing, information from clients and the company is shared via virtual data centers [2].

Cloud computing presents a practical avenue for achieving evident cost benefits, potentially transforming a data center from a fixed-cost environment into a dynamic pricing structure [3]. This technology has become apparent in the last few years and is expected to become a major trend soon. Cloud computing has several challenges and is linked to modern security flaws because of its novelty [4]. The model of cloud computing has experienced rapid and significant evolution, bringing about profound changes in the information technology industry. This evolution offers substantial cost savings and novel business opportunities for both providers and customers, thereby revolutionizing the industry. Cloud infrastructure is transforming the conventional model of IT service delivery. Thanks to its capabilities (such as shared resources, wide network access, self-service on-demand, etc.), the cloud has completely changed how computing infrastructure is abstracted and used, making cloud computing attractive [5].

Cloud computing provides an opportunity for cloud application connected to the internet for the purpose of remotely storing and accessing cloud data [6]. Users can choose cloud services to store their metadata on the cloud data server [7]. Cloud service providers are responsible for retrieving or managing the data kept at the cloud data center. Therefore, the collection of data for processing in a cloud data center should be executed with the highest level of professionalism.

Several studies work mention security issues related to cloud computing; nonetheless, there might not be enough thorough analyses that concentrate on the security consequences of multi-tenancy. An aspect that may need more research is how shared resources across several tenants affect security issues on different levels. Current available literature may not adequately address how security measures should be adjusted in real-time to emerging threats, given the agility and ongoing innovation of malicious actions aimed at cloud infrastructure. Not enough attention may be devoted to realizing how security flaws at one level can affect others and suggesting coordinated fixes. There can be gaps in the literature on the particular difficulties brought on by different international rules given the growing emphasis on data privacy and regulatory compliance. It may be necessary to conduct more research to determine how cloud infrastructure may guarantee compliance with various data protection rules.

The most significant hurdle is security, and worries about cloud computing persist with the ongoing emergence of numerous advancements in cloud computing platforms [8]. Following the COVID-19 pandemic, it is clear that more and more people and companies are adopting cloud services, software, and infrastructure because of its accessibility from anywhere at any time. Numerous research efforts and advancements, as highlighted in [9–12], have been put forth to address security risks. Many current security methods designed to safeguard the cloud lack a specific focus on emerging security risks within the cloud computing infrastructure. Consequently, these techniques are unable to recognize such attacks or vulnerabilities coming from the cloud service provider or the end user. Furthermore, the different layers of cloud infrastructure have not been thoroughly examined in a large number of previous research. This paper conducted an extensive assessment on the difficulties faced by the cloud computing infrastructure across several levels, including the application, host, network, and data levels, in recognition of the vital relevance of addressing these concerns.

2. Background of Cloud Computing

The emergence of cloud computing is a new development that refers to some previous ideas while drawing on innovative industry, technological, and environmental viewpoints. The roots of cloud computing can be traced to the 1950s, specifically the notion of "time-sharing," where multiple individuals would jointly access content and processing power. The term itself was coined in 1997 during a discussion on a "modern computing model" by Ramnath Chellapa, a professor at the University of Texas. Additionally, in the 1960s, John McCarthy introduced the idea of cloud computing, envisioning computing as a potential public resource in the near future [13].

Cloud computing was defined by the National Institute of Standards and Technology (NIST) in 2011 and was described as a paradigm that allows for easy, broad, and on-demand network access to a shared pool of flexible computing resources [14]. These resources, which include servers, storage, services, apps, and networks, may be quickly supplied and delivered with the least amount of assistance or administration work required from service providers. Figure 1, derived from the study in [15], illustrates the five key components of this cloud paradigm. Additionally, there are four deployment techniques and three service delivery types included. [5].

The purpose of cloud security frameworks is to guarantee the availability, confidentiality, and integrity of an organization's data in a cloud environment. conducted a comprehensive analysis to determine whether new security frameworks could improve cloud security. The goal of the study is to examine and compare different cloud security frameworks and standards in order to determine their overall impact on enhancing cloud security posture as well as its advantages and disadvantages. Several well-known cloud security frameworks were thoroughly examined by the authors, including the ISO/IEC 27017:2015 Cloud Security Controls, the NIST Cloud Computing Security Reference Architecture, and the Cloud Security Alliance (CSA) Security Guidance. The evaluation of these frameworks was conducted based on their capacity to address significant issues related to cloud security, including encryption, data protection, access control, and incident response.

Di Giulio's study contributes to the body of knowledge by providing a thorough analysis of cloud security frameworks and standards. It is an excellent tool for academics and practitioners who wish to make informed judgments on cloud security adoption and grasp the advantages and disadvantages of different security frameworks. According to Gartner lists, security/privacy, choosing a cloud environment, and governance as the three main challenges in cloud computing. The board of directors should oversee cloud investments to reduce risk, control costs, and turn a profit.

2.1. NIST's 5 Essential Cloud Computing Characteristics

The National Institute of Standards and Technology (NIST) has identified five key features of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

On-Demand Self-Service

It is considered the most important and vital features of cloud computing. This allows the client to continually monitor the server's capacities, uptime, and allotted network storage. One important aspect of cloud computing is that customers can customize the processing power to meet their requirements.

Broad Network Access

Broad Network Access is another crucial component of cloud computing. Networks and a range of portable devices, including laptops, desktop computers, tablets, and mobile phones, can access cloud services. Private clouds rely on local area networks, whereas public clouds use the internet. The quality of service in cloud computing, particularly in terms of broad network access, is significantly influenced by factors like latency and bandwidth.

Resource Pooling

Resource pooling stands out as a fundamental aspect of cloud computing, signifying the capability of a cloud service provider to distribute resources across numerous clients, tailoring services to meet individual requirements. This approach applied to services like data storage, processing, and bandwidth delivery, embraces a multi-client strategy. The real-time allocation of resources by the administration process ensures a seamless client experience without conflicts.

Rapid Elasticity

Cloud services offer the flexibility of elastic provisioning and release, often automated, enabling customers to rapidly scale according to demand. The provisioning capabilities are virtually limitless, allowing customers to access and utilize these capabilities at any time and in any desired quantity. Additionally, customers have the freedom to scale their cloud usage, capacity, and expenses without incurring additional contracts or fees. Rapid elasticity eliminates the need for purchasing computer hardware, as customers can leverage the cloud provider's computing resources.

Measured Service

Measuring capabilities in cloud systems improve resource consumption at an abstraction level appropriate for the particular service type. This measurable service covers a number of features, including users, processing, bandwidth, and storage. Under the pay-as-you-go concept, customers are billed according to their actual consumption. The transparent experience for both service consumers and providers is achieved through continuous monitoring, control, and reporting of resource usage.

2.2. Benefits of Cloud Computing

Cloud computing enables users to remotely access applications and data from any location and at any time using online devices like laptops or mobile phones. Additionally, cloud systems furnish the necessary infrastructure for businesses to create and launch enterprise software and services, enhancing agility and reducing time-to-market in software development. Furthermore, cloud systems present various advantages compared to traditional on-premises computing.

Resiliency and Availability

Resilience in the context of cloud computing denotes a service's capacity to promptly recover from disruptions. Measured by how quickly servers, databases, and networks can be restarted and recovered from any kind of damage, cloud resiliency is determined to be effective. Cloud services make duplicates of saved data as a safety measure against data loss. In case one server experiences data loss, the replicated version from another server is employed for restoration. A connected and essential concept in cloud computing is availability. The advantage of cloud services lies in their remote accessibility, eliminating geographical constraints when utilizing cloud resources.

Cost Reduction

The adoption of a "pay-as-you-go" payment model empowers organizations to manage their IT expenses by only paying for the resources they actively utilize. Additionally, there is no need for the acquisition or upkeep of their equipment, resulting in diminished capital expenditures (CAPEX) and a decreased total cost of ownership (TCO).

Security of Data

The majority of public clouds provide robust security features, including fine-grained permissions and access controls, authentication, encryption, API keys, and virtual private clouds (VPC) to safeguard sensitive data. Furthermore, the implementation of networked backups serves to mitigate the possibility of losing data.

Multiple Control Choices

The availability of various "as-a-service" cloud alternatives, such as SaaS, IaaS, and PaaS (representing software, infrastructure, and platform as a service), enables organizations to select their preferred level of control within the cloud environment.

Multiple Storage Options

Businesses have the flexibility to opt for public, private, or hybrid cloud storage solutions based on their specific needs and security requirements.

Facilitating Remote Work

Cloud computing makes remote work easier by allowing users to quickly and securely access company data via laptops and smartphones, among other devices. Using the cloud's capabilities, remote workers may carry out their duties and communicate with each other and with effectiveness.

2.3. NIST's Cloud Computing Stakeholders

The primary section of the NIST SP 500-292 outlines five primary roles within a model for cloud computing architecture., as shown in Table 1.

Table 1. Cloud Stakeholders

Stakeholders in Cloud	Definition
Cloud Consumer	The active subscribers acquire services and utilize the system, incorporating them into their operational expenses from service providers [16].
Cloud Provider	Service providers own and operate cloud computing systems, providing services to external parties. These providers take on the responsibility of system maintenance and upgrades. Examples of such providers include Microsoft, Google, IBM, Amazon, Oracle, and Sun [16].
Cloud Auditor	A cloud auditor is an external entity that assesses the controls implemented by providers of cloud computing services.
Cloud Broker	A Cloud Broker is an organization that oversees the utilization, effectiveness, and provision of cloud services, as well as facilitates interactions between providers and consumers of cloud services. Boomi, AWS Service Broker, Wipro BoundaryLess Enterprise (BLE), IBM Cloud Broker, etc.
Cloud Carrier	The intermediary facilitates connectivity and transportation of cloud services between cloud service providers and consumers. It enables access to cloud services through Internet networks, telecommunications, and various access devices [17].

2.4. Cloud Computing Services Delivery Models

Three primary models are used for delivering cloud services. The terms Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Despite the fact that they are all powered by cloud computing, each model functions uniquely and offers a wide range of services to businesses.

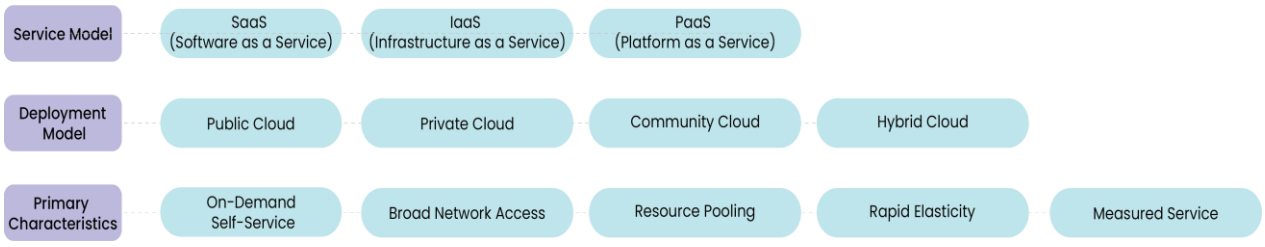

Fig.1. Cloud attributes and models

Software as a Service (SaaS)

SaaS stands out as the most recognized among the three cloud service delivery models, largely due to its widespread everyday usage by most individuals. Also referred to as "on-demand software," the SaaS delivery model allows users to reach fully operational software that is both managed and operated in the cloud. Furthermore, the SaaS model is linked with a pay-as-you-go feature, providing cloud consumers with a service that allows them to access the software through a web browser without dealing with complexities related to installation, upkeep, and significant initial expenses [18,19]. When individuals refer to "the cloud," they frequently mean SaaS applications such as Google Drive,

Dropbox, MS Office 365, Salesforce, or even services like Netflix.

Key Characteristics

- Regulated from a central location.
- Hosted remotely
- Accessible via the internet.
- Updates for software and hardware are not the users' responsibility. Updates are implemented automatically.
- Pay-per-use is the method of purchasing the services.

Infrastructure as a Service (IaaS)

Traditionally, companies maintained their IT infrastructure on-site, necessitating ongoing investments in costly hardware such as servers and storage, along with the responsibility of keeping everything current. With technological advancements, organizations increasingly sought assistance from cloud service providers to handle the management of their IT infrastructure. On-premises configurations gave way to cloud-based infrastructure as a result of the launch of Infrastructure as a Service (IaaS) on this date. With Infrastructure as a Service (IaaS), companies can leverage cloud servers' virtualized computing resources. Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Rackspace, DigitalOcean, Linode, and Cisco Metacloud are a few examples of LaaS.

Key Characteristics

- Resources are offered as a service.
- Dynamic and flexible.
- The scalability of the services is high.
- Automated administrative tasks.
- Access via a GUI and API.

Platform as a Service (PaaS)

Termed as a solution stack, this model of cloud service delivery is recognized as a Platform as a Service (PaaS). Programmers can create, test, run, and manage applications using the PaaS cloud computing platform. These platforms are supplied and maintained by an external vendor. Consequently, businesses are relieved from concerns related to tasks such as backups and server provisioning, as these responsibilities are handled on their behalf.

Key Characteristics

- Accessible to diverse users through a unified development application.
- Incorporates web services and databases seamlessly.
- Relies on virtualization technologies., allowing flexible scaling of resources based on organizational requirements.
- Supports multiple languages and frameworks.
- Enables automatic scaling capabilities.

Table 2. Below table shows the difference between SaaS, IaaS, and PaaS

Software as a Service (SaaS)	**Infrastructure as a Service (IaaS)**	**Platform as a Service (PaaS)**
It delivers web-based software and applications for fulfilling business responsibilities.	It offers a virtualized data center for storing data and establishing environments for the creation, examination, and implementation of applications.	It provides virtual platforms and tools for application development, testing, and deployment.
It gives users access to software as a service.	It provides access to a variety of resources, including virtual storage and computers.	It provides tools and runtime environments for app deployment.
It is used by end users.	It is used by network architects.	Developers use it.
SaaS provides Infrastructure+ Platform +Software.	IaaS provides only Infrastructure.	PaaS provides Infrastructure + Platform.

2.5. Cloud Computing Deployment Models

The NIST definition of cloud computing encompasses four deployment models that represent distinct types of cloud environments. Users have the flexibility to select the model that aligns with their requirements and preferences in terms of features and capabilities. The initial crucial step in the implementation process is to carefully select the appropriate type of cloud for an institution, ensuring a successful implementation [20]. As stated in [21], institutions that faced challenges in deploying a model often did so due to selecting an inappropriate type of cloud. To reduce the risk of failure, institutions should assess their data before determining the best cloud form. Four fully integrated models for each sort of cloud-based system are based on the administrative requirements and data senility. The public, private, community, and hybrid cloud are some of these models.

Public Cloud: The public cloud provides easy accessibility to systems and services for the general public. However, its openness may lead to reduced security, as seen in applications like email.

Private Cloud: A private cloud enables systems and services to be accessed exclusively within an organization, ensuring heightened security due to its restricted nature.

Community Cloud: A community cloud enables a particular set of organizations to have access to certain systems and services.

Hybrid Cloud: A combination of public and private clouds is known as a hybrid cloud. Under this configuration, non-essential tasks are carried out on the public cloud and critical tasks are carried out on the private cloud.

2.6. Existing Surveys

A study conducted by [22] highlighted the security challenges associated with data transfer within a cloud environment. The survey not only identified potential threats but also proposed practical solutions to address them. In [23], a survey presented a comprehensive taxonomy of cloud services, categorizing them based on cloud infrastructure vendors and revenue. Different categories, including computing, networking services, databases, storage, analytics, and machine learning, were included in the taxonomy. The core components of cloud computing, including computing, networking, and storage, were noted for their robust functionality across all cloud vendors. On the other hand, different cloud suppliers offered different possibilities when it came to streaming, data processing and orchestration, building blocks, and machine learning through their databases, machine learning, and data analytics solutions.

One survey, covered in [24], focused on the security issues that cloud ecosystem entities face. These parties included the data owner, the cloud service provider, and the cloud customer. The study also focused on the cloud's cryptographic features, which include storage, communication, and service-level agreements. In addition, the study included necessary updates to look at the causes and effects of various cyberattacks.

Research conducted by [25] examined data protection concerns within a multi-tenant system in cloud computing and proposed strategies to handle security challenges. However, this survey placed a greater emphasis on data privacy as opposed to security.

Research presented in [26] offered a precise definition of cloud computing and delineated the various layers of cloud architecture. Furthermore, the study conducted a comparative analysis of three service models, namely SaaS, PaaS, and IaaS, in conjunction with deployment models encompassing private, public, and community clouds. The authors explored the information security prerequisites specific to private and public cloud environments. Additionally, they delved into the primary concerns and obstacles associated with security in the realm of cloud computing.

A survey detailed in [27] concentrated on the identification of various threats commonly encountered in cloud computing settings. The author's primary contribution to this paper lies in categorizing threat types according to service resources within the cloud context. The classification was established based on the description and scope of these threat types.

A research study on the design of cloud computing environments and software-defined networks (SDNs) with regard to detection methods and Distributed Denial of Service (DDoS) attack scenarios was conducted in [28]. Furthermore, this survey investigated the creation of experimental environments and the utilization of simulation tools for both DDoS attacks and their detection.

In the examination conducted by [29], a survey systematically assessed prominent attacks directed at the security of Cloud Computing. In addition to reviewing these threats, the study offered suggested remedies and defenses with the goal of creating a standard for comparative analysis. However, the research was noted for its absence of methodologies to address certain significant security challenges.

In [30], a comprehensive survey outlined security concerns and prerequisites applicable to cloud computing while identifying threats and well-known vulnerabilities. The study introduced a novel categorization of contemporary security solutions within this domain. It outlined a set of documented policies, procedures, and processes, offering a framework for secure cloud environment management aimed at identifying vulnerabilities and enhancing confidence in an increasingly interconnected world.

Prioritizing privacy concerns, the researchers in this study [31] reviewed technologies that enable the outsourcing of sensitive data processing and storage to public clouds. In particular, the study looked at data splitting and anonymization strategies for disguising outsourced data in addition to cryptographic techniques that have been covered in other surveys. Based on how well these approaches supported operations using masked outsourced data, how much they cost, and how they affected data management, they were compared.

A thorough end-to-end mapping of cloud security requirements, including the identification of threats, known vulnerabilities, and recommended fixes, was provided in a narrative evaluation carried out by [32]. In addition to helping to thorough end-to-end mapping, the study helped create a common taxonomy for security needs, threats, vulnerabilities, and responses. Furthermore, the assessment clarified security issues in associated fields such as cloud-enabled big data applications, Internet of Things (IoT), software-defined networking (SDN), network function virtualization (NFV), and trust-based security models.

The study described in [33] conducted a thorough literature assessment of the literature on cloud computing and trusted computing integration for Infrastructure as a Service (IaaS). In order to create a novel Infrastructure as a Service (IaaS) architecture and promote more confidence between cloud service tenants and cloud service providers, the combination of cloud computing with trusted computing was investigated.

In [34], the authors delved into the predominant security challenges in contemporary cloud computing and offered optimal practices for both service providers and organizations seeking to oversee cloud services effectively. Notably, many of the surveys discussed concentrated solely on specific layers of the cloud infrastructure. For example, surveys like [22, 23, 26, 32] addressed issues solely at the data level, while [24] focused exclusively on the application level. Furthermore, [29] surveyed the network level, and another paper [30] specifically targeted the host level.

Some research efforts have been undertaken across multiple levels of cloud infrastructure, as evident in studies like [35, 25, 28]. Additionally, works such as [24, 31, 33, 36] have taken a comprehensive approach by considering all levels of infrastructure. However, [23] exclusively examined the public cloud and focused on cloud services concerning infrastructure vendors and revenue. In contrast, [31] concentrated on the management of data within the public cloud. It's worth noting that [33] took the form of a narrative review without conducting analyses of the reviewed materials. Lastly, the survey presented in [36] was confined to analyzing security strictly from the provider's perspective.

To summarize, the existing survey studies on the security of cloud infrastructure are not very thorough since they frequently do not cover the security elements of host, network, application, and data levels of cloud infrastructure. A portion of the polls that have been reviewed only address one or more of these levels. Furthermore, some polls neglect to take into account the opinions of both service providers and clients. Our proposed survey, in contrast, stands out because it thoroughly examines problems at all cloud computing infrastructure levels, offers in-depth analyses of these problems, investigates current mitigation strategies, and, in the end, highlights problems and challenges that remain unresolved while providing suggestions for further research.

2.7. Cloud Security Problems and Solutions

Cloud computing has completely changed how businesses handle, store, and use apps and data. But as Figure 1 illustrates, this paradigm change has brought out a number of security issues that must be resolved to guarantee the privacy, availability, and integrity of data in the cloud.

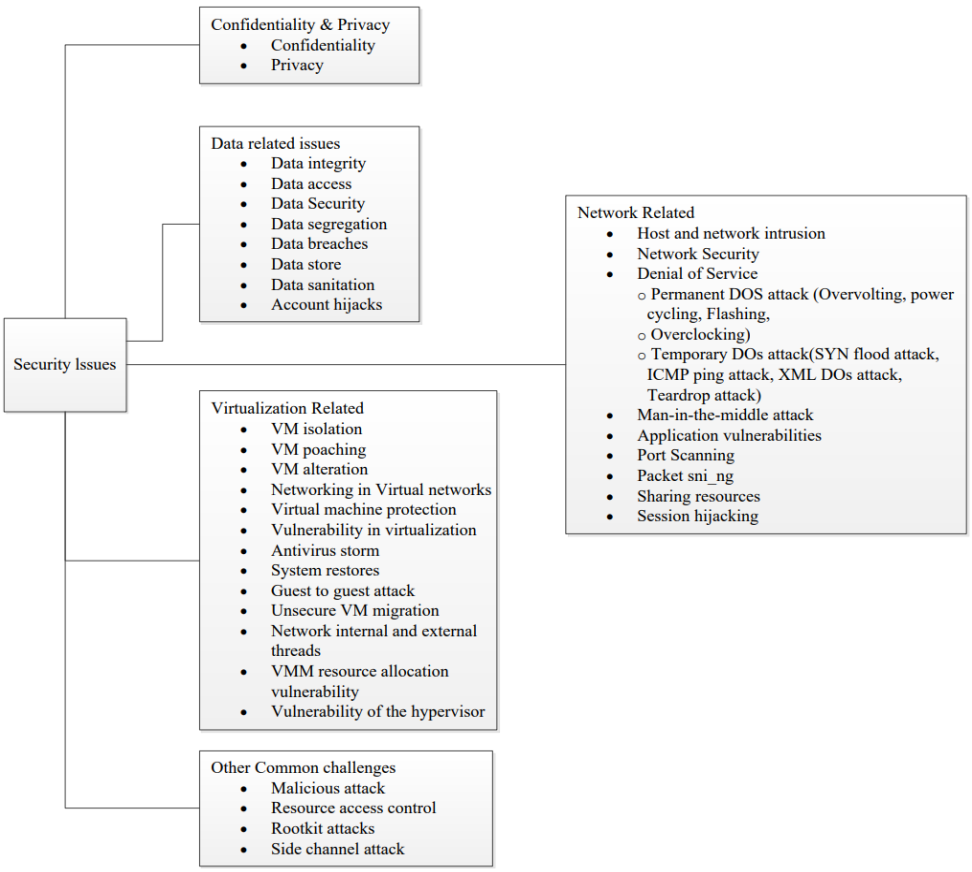

Fig.2. Main components of cloud security issues

A. Cloud Security Problems

Data Privacy and Leakage: When cloud environments are shared, there are privacy problems. Sensitive information may leak as a result of unauthorized access or data breaches.

Data Location and Jurisdiction: While cloud infrastructures are dynamic, it might be difficult to pinpoint the precise location of data, which could result in legal disputes and inconsistencies with data protection laws.

Multi-tenancy Risks: Risks associated with multi-tenancy include the possibility of resource and data co-residency,

in which data from several clients may reside on the same physical hardware and might expose that data.

Inadequate Access Control: In cloud systems with complicated access requirements, it can be difficult to ensure appropriate access control mechanisms to prevent unauthorized users from accessing resources and data.

B. Cloud Security Solutions

Multiple strategies have been proposed and used to address the problems and mitigate the risks associated with cloud security. Here are a few illustrations.

Key management and encryption: Data that is encrypted both in transit and at rest is more shielded from unwanted access. Maintaining the security of encryption techniques requires the use of appropriate key management solutions.

Identity and Access Management (IAM): Managing user identities, roles, and permissions requires strong IAM solutions. Possible risks are reduced when the least privilege concept is put into practice.

Virtualization Security: In order to stop attacks that aim to exploit weaknesses in the hypervisor or virtual machine instances, the virtualization layer must be properly secured.

Security Monitoring and Incident Reaction: The ability to identify and respond promptly to security issues is made possible by the application of comprehensive security monitoring technologies and procedures. Threat intelligence, log analysis, and ongoing monitoring are all essential for identifying and minimizing security breaches.

Cloud-specific Security Tools: In the cloud context, using cloud-native security tools helps improve threat detection and response. Real-time monitoring is provided by programs like Azure Security Center and AWS GuardDuty.

Cloud Security Standards and Certifications: A framework for assessing and guaranteeing the security of cloud services is provided by industry-recognized security standards and certifications. The CSA STAR, FedRAMP, and ISO 27001 standards help enterprises assess the security capabilities of CSPs. Organizations are helped by routine security audits and assessments to find vulnerabilities and make sure security rules are followed. Vulnerability scanning, penetration testing, and independent audits are components of a proactive security approach. putting in place secure configurations for cloud services and hardening the underlying infrastructure to reduce potential vulnerabilities

In previous literature, certain gaps have been noted. One area of vulnerability in cloud security research is the need for a comprehensive understanding of the growing risks and threats associated with cloud systems. The ever-evolving cloud ecosystem gives rise to new attack vectors and vulnerabilities, thus staying ahead of potential threats requires ongoing research.

3. Cloud Computing Infrastructure Security Concerns

Innovations in cloud computing have transformed the operational landscape for businesses. From data collection and storage to interconnected and efficient workflows to rapid scalability, these advancements provide significant benefits that enhance processes, facilitate flexible and sustainable expansion, elevate customer experiences, and enhance competitiveness, among various other advantages.

Nevertheless, as an increasing number of organizations depend on cloud-based technologies for conducting business—a reported 94% of enterprises utilizing a cloud service—leaders must prioritize investments in securing their systems against cyberattacks and other potential threats [37].

Businesses need to take into account the diverse security threats linked with cloud computing alongside the numerous benefits. Experts emphasize that companies relocating their data and operations to the cloud without a well-defined strategy that considers potential drawbacks face challenges later on. Furthermore, prominent cloud security breaches can have detrimental effects on a company's financial standing and reputation.

Cloud service providers consider it a shared obligation to manage the dangers and difficulties brought on by cloud security issues. The security of the customer's data stored in the cloud falls under their purview. Simultaneously, the cloud service provider assumes complete responsibility for securing the cloud infrastructure. Whether the service is software-as-a-service (SaaS) like Microsoft Office 365 or infrastructure-as-a-service (IaaS) like Amazon Web Services (AWS), users are always responsible for managing access to and protecting their data from security threats.

Cloud data security is a crucial factor in most security issues in cloud computing. The primary focus of these concerns is the data that users upload to the cloud. Whether it is caused by data theft, a lack of control over the data, or something else entirely. Several security problems related to cloud computing must be considered when integrating cloud technology, and solutions must be put in place.

3.1. Cloud Security Levels

Cloud computing security operates on various levels [38], aiding both organizations and Cloud Service Providers (CSPs) in the implementation of security measures. These levels can be categorized broadly as follows:

A. Physical Security Level

Organizations that possess their own data centers or Cloud Service Providers (CSPs) offering dedicated cloud services must establish security measures at this foundational level. On a physical level, protecting the grounds around

the data centers entail hiring security guards, enforcing access controls, logging critical visitor data, and instituting comparable procedures throughout the region. This level is vulnerable to malicious attacks by people inside or outside the company, mistakes involving people, and natural or man-made disasters resulting in harm to the infrastructure.

B. Host/Virtualization Level

Virtualization serves as a core component of Cloud computing, with Cloud Service Providers (CSPs) utilizing virtualized environments to deliver services to diverse users. CSPs are unable to disclose information about the virtual images and operating systems they employ. Security at the virtualization level is crucial due to potential intrusion attempts originating from the hypervisor. [39] Hypervisors represent a singular point of security vulnerability. If an attacker successfully hijacks one hypervisor, it poses a substantial risk to the entire cloud system [40].

C. Network Security Level

Networks play a crucial role as connectors in cloud computing, serving as the means through which users connect to cloud services and data communication takes place. Because there are so many different kinds of assaults that could affect the network, including active and passive ones that might compromise availability, confidentiality, and integrity, network security is crucial. Prioritizing the deployment of reliable and secure network communication protocols is imperative for cloud service providers [41,42].

D. Interface Security Level

The operating system that these services are provided on as well as the UI for the services itself must be secured. Cloud service providers (CSPs) commonly employ Linux as an operating system since it is an open-source platform with superior security compared to other operating systems. For instance, Linux powers IBM Bluemix, a cloud service, while Windows powers Microsoft Azure [43].

E. Operating System Security Level

The operating system plays a vital part in the cloud host machine. Except for bare-metal hypervisors, all hypervisors have an operating system. Operating system security is important since every virtual machine is built on top the operating system. Compromising the operating system poses a substantial risk, potentially placing all virtual machines within the attack zone.

F. Database Security Level

Data is an invaluable resource for every kind of organization. When users switch to cloud services, it could be necessary for the Cloud Service Provider (CSP) to store data. Understanding the importance of data at rest on CSP servers is essential. Only 8.4% of CSPs do not encrypt data while it is at rest, despite the fact that the majority do so during data transit. Databases need an extra layer of protection when they deal with sensitive data, like financial institutions [42, 44, 45, 46].

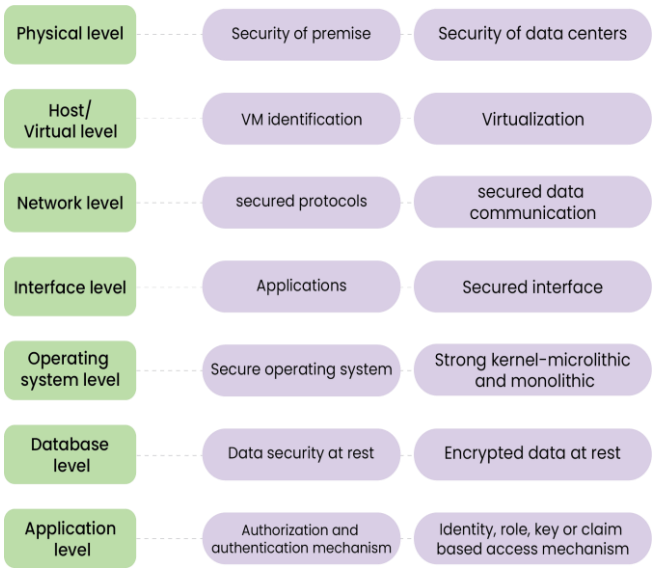

Fig.3. Security Levels in cloud computing

G. Application Security Level

The application security level serves as the final tier of security. It determines the authorized access to services and how access is granted. At this security level, the goal is to prevent attackers from gaining control over hardware and

applications. Identity, role, key, or claim-based access techniques are used by cloud service providers (CSPs) to guarantee this. These methods ascertain the specific areas of services visible to different types of users, mitigating the risk of both unintentional and intentional data theft, along with active or passive attacks on services [47,48].

3.2. Cloud Security Issues: Risks, Threats and Challenges

Cloud environments pose distinct risks, threats, and challenges that require careful consideration. Recognizing the subtle distinctions among these factors is essential for effective resource allocation, response strategies, risk management, and informed decision-making.

A. Cloud Security Risks

It is not possible to eliminate risk; instead, our goal is to effectively manage it. Being aware of common risks in advance enables us to proactively address and handle them within our environment.

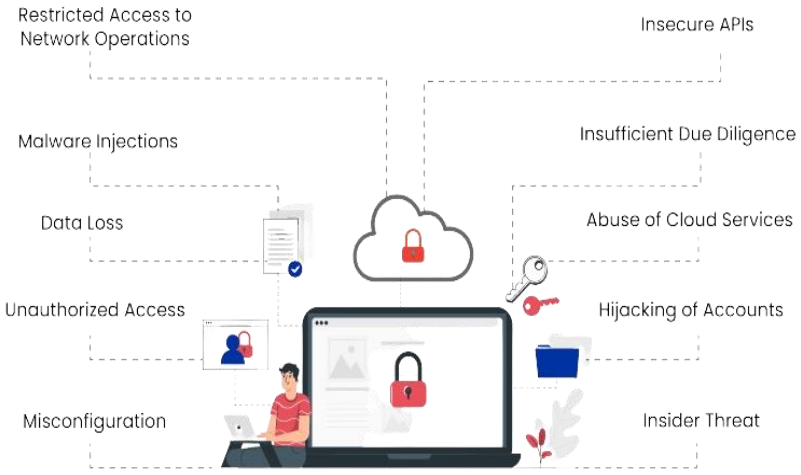

Fig.4. Cloud security risks

a. Misconfiguration

One of the main causes of data breaches is clearly incorrect cloud security configuration. Due to a lack of comprehensive cloud security posture management methodologies, many organizations' cloud-based infrastructure is left open to vulnerability.

There are multiple reasons that lead to this vulnerability. Because cloud infrastructure is meant to be user-friendly and facilitate data sharing, it can be difficult for businesses to make sure that only authorized individuals can access their data. Furthermore, companies that use cloud-based infrastructure do not have total access or control over their systems; instead, they must setup and safeguard their cloud deployments using security measures that are supplied by their cloud service provider (CSP). Misconfigurations or security oversights can readily expose an organization's cloud-based resources to prospective attackers, given the increasing frequency of multi-cloud deployments with variable vendor-provided security controls and the unfamiliarity of many enterprises with securing cloud infrastructure.

b. Unauthorized Access

While an enterprise's on-premises infrastructure, its cloud-based installations are immediately accessible from the public Internet and operate outside of the network perimeter. Although this makes an organization's cloud-based resources more accessible to both customers and employees, it also increases the possibility that attackers will get unauthorized access to them. Attackers may be able to obtain direct access, sometimes without the organization's knowledge, through improperly set security mechanisms or credential compromise.

c. Data Loss

The possibility of data loss, sometimes known as a data leak, is a common problem with cloud computing. If the security of a cloud service is compromised, those who have access to sensitive data, such as employees and business colleagues, provide hackers with a way to potentially compromise sensitive data or private information.

When organizations adopt cloud computing, they relinquish a portion of control to the Cloud Service Provider (CSP). Consequently, individuals outside the IT department may assume responsibility for safeguarding critical company data. In the event of a breach or attack on the cloud service provider, the company faces the prospect of losing data, intellectual property, and potential liability for ensuing damages.

A recent study from the French multinational Thales, which specializes in information security and defense, states that in 2023, 40% of enterprises had a data breach in their cloud environment, up from 35% in 2022. According to the

survey, human error is the main reason behind 55% of cloud data breaches [49].

d. Malware Injections

Malware injections involve the incorporation of scripts or segments of code into cloud services, disguising themselves as "legitimate instances" while operating as Software as a Service (SaaS) from cloud servers. This suggests that malicious malware may find its way into cloud services and manifest itself as a necessary component of the application or service running on the cloud servers.

Once the malware injection is finished, attackers can work with the cloud to steal data, compromise the security of personal information, and eavesdrop. In its analysis of the dangers and weaknesses connected to malware installations on cloud security, East Carolina University's report on security threats in cloud computing concludes that "malware injection attacks have emerged as a significant security concern in cloud computing systems."

e. Restricted Access to Network Operations

Limited visibility into network operations is a disadvantage of moving from an on-premises data storage architecture to a cloud-based infrastructure. Organizations grant varying degrees of control over their IT infrastructure to Cloud Service Providers (CSPs) in exchange for benefits such as cost savings and scalable storage through on-demand provisioning. The absence of visibility in cloud computing is another serious security concern.

The extent of control that CSPs possess and the data security responsibilities of enterprises depend on the service model adopted. Nonetheless, the ongoing threat posed by the absence of insight into cloud environments persists for companies relying on them for the management of mission-critical data, regardless of the shared responsibility model.

f. Insecure APIs

Application Programming Interfaces (APIs) provide customers the ability to customize their experience with cloud security tools. However, the inherent nature of APIs introduces potential threats to cloud security. APIs handle authentication, access permissions, and encryption, empowering businesses to tailor the functionalities of their cloud-based infrastructure services to meet specific business needs.

As the API infrastructure grows in order to provide more services, the security threats increase. APIs give developers the power to write original programs and easily incorporate them with other necessary applications. When it comes to integrating YouTube content into websites or applications, developers can use YouTube as a well-known and simple example of an API. Applications' interactions with one another are where an API can be vulnerable. While companies and developers gain from this flexibility, there is a risk to their security as cloud users.

g. Insufficient Due Diligence

Though a lot of the issues that have been covered thus far have been technological in nature, this security vulnerability occurs when an organization does not have a well-defined plan for its objectives, assets, and solutions within the context of cloud security. It is, to put it another way, a component focused on people. A corporation may be exposed to potential cloud computing security risks if it rushes into a multi-cloud deployment migration without careful planning and consideration for whether the services will fulfill user expectations. This is especially important for companies handling customer financial data or data covered by PCI, FERPA, PCI-DSS, and PII rules.

h. Abuse of Cloud Services

With the expansion of cloud-based services, both small and large businesses can easily store vast amounts of data. However, the unprecedented storage capacity of the cloud also means that malicious software, unauthorized applications, and other digital assets can be hosted and distributed by both authorized users and hackers. This practice can have repercussions for both the cloud service provider and its clients. For example, privileged users may violate the terms of the service provider, directly or indirectly increasing cloud computing security risks.

i. Account Hijacking

The expansion and widespread adoption of cloud security tools by many enterprises have introduced a new set of challenges related to account hijacking. Attackers now can remotely access sensitive data stored in the cloud using login details belonging to you or your employees. They can manipulate and falsify data using hijacked credentials. In 2023, a misconfigured Amazon S3 bucket exposed the personal data of 119 million individuals. During the same year, an attacker exploited a zero-day vulnerability to pilfer credentials from a cloud-based identity provider, affecting millions of users.

Traditional cloud security threats like phishing, keylogging, and buffer overflow attacks persist. However, a notable emerging threat is the Man in the Cloud Attack, where attackers steal tokens leveraged by cloud service providers to authenticate individual devices without requiring logins for each update and synchronization. These tokens can grant unauthorized access to cloud accounts and data.

j. Insider Threat

While an internal attack on your company may appear unlikely, the insider threat is a real concern. Employees who

possess authorization to use cloud-based services offered by their employer run the risk of misusing or gaining access to private information such as financial records, client accounts, and other vital data.

B. Cloud Security Threats

A threat refers to an attack directed at your cloud assets to exploit a recognized risk.

a. Zero-day Exploits

A zero-day exploit is a kind of cyberattack that takes use of an unpatched or previously undiscovered vulnerability in computer hardware, firmware, or software. The phrase "zero-day" refers to the fact that the software manufacturer has no time to address the vulnerability since hackers can take advantage of it right away to infiltrate systems that are susceptible.

The term "zero-day" is sometimes written as "0-day," and it is often associated with the word's vulnerability, exploit, and attack [50]. Here's a breakdown of these terms:

Zero-day Vulnerability

- A software fault or weakness that is found by attackers before the program provider is made aware of it is referred to as a zero-day vulnerability.
- Because vendors are unaware of this vulnerability, there is no patch or fix available, making systems susceptible to attacks.

Zero-day Exploit

- Hackers use a technique known as a zero-day exploit to target systems by taking advantage of an undiscovered vulnerability.
- It is a particular code or method that compromises a system by exploiting a zero-day vulnerability.

Zero-day Attack

- Using a zero-day exploit to harm or gain unauthorized access to a system that is compromised by a zero-day vulnerability is known as a zero-day attack.
- Attackers leverage the exploit to carry out malicious actions, such as stealing data or disrupting system functionality.

Developers strive to produce a patch as soon as a vulnerability is discovered in order to stop possible attacks. However, the discovery of security vulnerabilities is not immediate, and there can be a significant lag before developers identify the specific vulnerability that was exploited in an attack. The timeframe for discovery can range from days to weeks or even months. Even after the identification of a vulnerability and the release of a zero-day patch, not all users promptly implement the patch. In recent years, hackers have demonstrated a tendency to exploit vulnerabilities swiftly after discovery, sometimes outpacing users' ability to apply patches.

Once an exploit is discovered, and a patch is released and applied, the term "zero-day threat" is no longer applicable. Zero-day attacks pose a heightened level of danger because only the attackers are initially aware of them. Upon infiltrating a network, criminals can choose to launch an immediate attack or patiently wait for an opportune moment to maximize the impact of their actions.

A zero-day hack has the potential to exploit vulnerabilities in various systems, including:

- Hardware and firmware
- Office applications
- Web browsers
- Operating systems
- Open-source components
- Internet of Things (IoT) devices

b. Advanced Persistent Threats (APT)

An advanced persistent threat (APT) refers to a comprehensive term used to characterize an orchestrated attack campaign in which an intruder or a group of intruders establishes an unauthorized and enduring presence within a network. The primary objective of such an attack is to clandestinely access and gather highly sensitive data over an extended period.

The entire purpose of an Advanced Persistent Threat (APT) attack involves a sequence of five stages:

Stage One: Gain Access

Similar to a burglar leveraging various means such as network vulnerabilities, infected files, phishing emails, or exploiting application vulnerabilities, cybercriminals aim to gain entry into a targeted network by introducing malware.

Stage Two: Establish a Foothold

Cybercriminals install malware at this point to make it easier to build a network of tunnels and backdoors. These serve as covert pathways, allowing them to move within the systems undetected. Techniques like code rewriting may be employed to obfuscate their activities.

Stage Three: Deepen Access

Once inside the network, hackers employ methods like password cracking to escalate their access, obtaining administrator rights. This elevated level of access provides greater control over the system.

Stage Four: Move Laterally

With administrator rights secured, hackers can freely navigate within the system, attempting to access other servers and secure areas of the network.

Stage Five: Look, Learn, and Remain

Having gained deep access to the system, hackers thoroughly understand its workings and vulnerabilities. This knowledge allows them to extract desired information at will. The APT attackers may choose to maintain this presence indefinitely, continuously observing and learning or withdrawing after achieving specific objectives. They often leave a concealed backdoor for potential future access.

c. Insider Threats

Insider threats are cybersecurity vulnerabilities that come from those who have been granted authorized access, such as partners in business, contractors, and employees. These people might misuse their authorized access—intentionally or inadvertently—or hackers could get access to their accounts.

Types of Insider Threats

Malicious Insiders

Malicious insiders typically consist of disgruntled current employees or former employees who retain access credentials. These individuals intentionally exploit their access for motives such as seeking revenge or financial gain. In certain cases, malicious insiders collaborate with external factors, such as hackers, competitors, or nation-state entities. Their collaboration aims to disrupt business operations by introducing malware, tampering with files or applications, or leaking sensitive information like customer data, intellectual property, and trade secrets.

Negligent Insiders

In contrast to malicious insiders, negligent insiders pose security threats inadvertently, lacking malicious intent. They acted carelessly or ignorantly when they fell victim to phishing scams, bypassed security measures to save time, misplaced a laptop that hackers could use to get into the company network, or sent private emails to people outside the company without realizing it.

Compromised Insiders

Legitimate users whose credentials have been stolen by outside threat actors are referred to be compromised insiders. As per the Ponemon research [51], insider risks originating from compromised insiders are generally the most expensive among all insider threats, with an average remediation cost of USD 804,997.

Insider acts that are careless often lead to compromised insider occurrences. For example, in 2021, a fraudster used a social engineering technique—more precisely, a voice phishing (vishing) phone call—to get login credentials for the trading platform Robinhood's customer support services.

d. Cyberattack

Any intentional attempt to gain unauthorized access to a computer system, network, or digital device with the intent to steal, expose, alter, disable, or destroy programs, data, or other assets is referred to as a cyberattack. Cyberattacks are executed using unapproved channels. Cyber threat actors launch these kinds of attacks for a variety of reasons, from small-time thievery to hostile conduct. These actors use a variety of strategies, such as social engineering frauds, malware assaults, and password theft, to gain unauthorized access to the systems they target.

C. Cloud Security Challenges

In rapidly expanding multi-cloud environments, challenges represent intricate issues related to cloud security that organizations may encounter. Many organizations find it difficult to manage complicated access-control lists, particularly when there are multiple clouds involved. A common cloud security issue is also making sure that various data protection laws are followed in a globally dispersed cloud infrastructure.

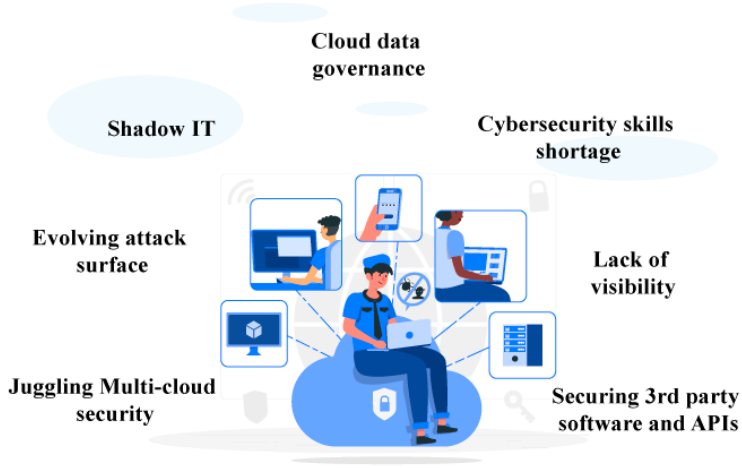

Fig.5. Cloud security challenges

a. Securing Third-party Software and APIs

Securing third-party software and addressing insecure APIs are crucial aspects of fortifying an enterprise's defense against cyber threats. Vulnerabilities in third-party software and APIs can potentially expand the attack surface, granting unintended access. A lot of businesses use third-party software to improve software development lifecycles (SDLC) and their cloud infrastructures. These third-party applications, integrated into SDLCs, interact through APIs, forming a vital component of the software supply chain. Proper attention and management are essential to safeguard the software supply chain from various cyber threats.

b. Lack of Visibility

SaaS, PaaS, and IaaS components are commonly used in a conventional cloud arrangement, which also occasionally incorporates on-premises data centers and hybrid models combining public and private clouds. The world of IT is complex; it involves digital identities, third-party applications, and many types of sensitive data in both transit and static phases. Diverse users can now quickly extend cloud environments, unlike in the past when only specific IT teams could commission additional cloud assets. It's critical to keep consolidated visibility without blind spots because new assets and dependencies are emerging across multi-cloud environments very quickly and extensively. Monitoring workloads, APIs, code technologies, CI/CD tools, security and identity tools, compute and data platforms, and code technologies are all included in comprehensive visibility. Both known and unknown security flaws have the potential to develop into serious security emergencies in the absence of centralized visibility and real-time monitoring. Inadequate visibility can also hinder incident response, resulting in longer times and more work.

c. Shortage of Cloud Security Experts

Insufficient cybersecurity expertise often compels businesses to heavily depend on external security solutions, such as SaaS products, to tackle security challenges specific to cloud environments. The absence of in-house cloud security professionals poses challenges in comprehending and addressing the intricate cybersecurity requirements of cloud-native IT environments. The necessity of shift-left efforts, which enable developers to proactively address security issues early in the software development life cycle (SDLC), is highlighted by this shortfall. The global scarcity of cybersecurity professionals has the potential to result in diverse outcomes, ranging from minor incidents to severe security breaches leading to financial losses and irreparable damage to reputation.

d. Cloud Data Governance

The significance of data as a paramount organizational asset cannot be emphasized enough. Robust governance and protection mechanisms are needed for valuable assets such as Personally Identifiable Information (PII), Protected Health Information (PHI), and Payment Card Industry (PCI) data that are stored in vast repositories of cloud data. Challenges in cloud data governance encompass:

- Establishing visibility across public buckets, and data volumes, and managed databases in AWS, GCP, and Azure.
- Detecting instances of data exposure.
- Understanding the flow and lineage of data.
- Implementing policies for effective governance.
- Ensuring adherence to compliance requirements.

Businesses must identify and remove any attack paths that could lead to sensitive data in cloud systems.

e. Shadow IT

Shadow IT is any hardware, software, or IT resource used inside a corporate network without permission from the IT department; it frequently occurs without their knowledge or supervision. Using a thumb drive or personal Dropbox account to share work files, holding meetings via Skype when WebEx is the official company platform, or starting a Slack group chat without first getting IT department permission are all examples of shadow IT in action.

Shadow IT specifically excludes malware or any other malicious assets deliberately introduced by hackers. Instead, it pertains solely to unsanctioned assets deployed by authorized end users within the network.

As per Cisco, approximately 80 percent of employees within a company engage in shadow IT practices. Employees frequently resort to shadow IT for the sake of convenience and productivity, believing that they can work more efficiently and effectively by utilizing their personal devices and preferred software, rather than relying on the company's approved IT resources.

This trend has only intensified with the increasing consumerization of IT and, more recently, the surge in remote work. Software-as-a-service (SaaS) facilitates the deployment of advanced IT systems for collaboration, project management, content creation, and other purposes by anyone with a credit card and minimal technical knowledge. Organizations bring your own device (BYOD) policies allow employees to utilize their personal computers and mobile devices on the corporate network. Despite the presence of a formal BYOD program, IT teams often face challenges in monitoring the software and services employees employ on BYOD hardware, and enforcing IT security policies on personal devices can be challenging.

f. Evolving Attack Surface

Cloud computing's economical and one-click scalability is one of its main benefits. But the cost of this scalability is an ever-widening attack surface. The growth in the amount of cloud assets—such as workloads, appliances, serverless components, virtual machines, data, and identities of people and services—is the primary cause of the increase. These cloud assets are vulnerable to a number of security risks, including password and credential weakness, misconfigurations, unintentional public disclosure of secrets and access keys, and overprivileged entitlements.

Rapidly expanding businesses can't afford to scale back operations to simplify their extensive cloud environments and narrow the attack surface. Thus, maintaining operational agility while managing the dangers associated with dynamic, ever-expanding attack surfaces is a major problem in cloud security.

g. Multi-cloud Security

Multi-cloud security is a holistic cloud security solution designed to safeguard and mitigate advanced security threats and cyberattacks targeting enterprise and customer data, assets, and applications. This approach extends protection across diverse cloud infrastructures and environments, ensuring comprehensive security measures.

The security hurdles in cloud computing encompass issues such as data governance, compliance, visibility, workload misconfigurations, IAM complexities, and malware threats. Organizations often acknowledge certain risks within their risk tolerance and counter more severe threats with robust cybersecurity measures. In multi-cloud infrastructures, managing IAM and access control stands out as a major security challenge. In essence, businesses must understand who has access to specific cloud resources and the reasons behind it. Without this comprehension, companies struggle to pinpoint vulnerabilities, foresee potential attack routes, and assess the potential impact of cloud security incidents.

4. Related Existing Solutions in Cloud Levels

This section lists and classifies numerous methods that have been proposed in the literature based on the four tiers of cloud architecture (data, application, network, and host). The following subsections go into further detail about these options.

4.1. Solutions at the Data Level

In the shift from traditional computing models to the Internet-based cloud model, there is a crucial emphasis on ensuring data security and privacy. The repercussions of data loss or leakage can have a significant impact on an organization's business and erode trust in its brand. A research study [52] explored the audit aspect within the cloud computing environment, with data auditing encompassing considerations such as data confidentiality, integrity, remanence, provenance, and lineage. With the exception of data remanence, which is still an open problem, especially in public cloud services, the study found a number of basic approaches for each of these factors that might satisfy cloud service users' expectations for data auditing. The study's findings demonstrated that cloud providers have given infrastructure security auditing precedence over data auditing, even though there are many strategies available to satisfy user auditing concerns in data auditing.

The authors of the study [12] suggested a hybrid layered approach that combines a lattice-based security technique with other measures to protect user data. The study presented a fresh way to use the lattice model to examine roles and

responsibilities. In order to improve sensitive data security, the AES and RSA algorithms were utilized.

A design for modeling data security in cloud computing was presented by the research in [53]. The study examined cloud storage data security at every level. The results show that most cloud storage follows a three-tier paradigm for cloud data security, with a fourth level for data integrity checks. Using Petri nets to explain each level of cloud data security, the article presented a four-level model for data security in cloud computing.

The research presented in [54] identified challenges associated with cloud data storage, including issues like data breaches, data theft, and unavailability of cloud data. The study put forth potential solutions to address these concerns, focusing on aspects such as identity management and access control. Despite these proposed solutions, there remain unresolved issues in access control and identity management, such as vulnerabilities like easily resettable weak credentials, the risk of denial-of-service attacks leading to temporary account lockouts, deficiencies in logging and monitoring capabilities, and potential XML wrapping attacks on web pages.

A hybrid approach was proposed by the research described in [55] with the goal of enhancing cloud data security by means of encryption techniques. To improve overall cloud security, the hybrid technique specifically incorporated blowfish with homomorphic encryption. However, practical implementation challenges were identified, primarily related to the slow and computationally expensive nature of homomorphic encryption, rendering it impractical for current use. Additionally, the blowfish algorithm, while employed in the hybrid approach, lacks authentication and non-repudiation capabilities since multiple individuals might share the same key. Moreover, drawbacks were noted in the decryption process of this method, leading to increased time and bandwidth usage.

The research presented in [56] employed elliptic curve cryptography (ECC) for encrypting data within the cloud environment, leveraging the small key size characteristic of ECC. The utilization of ECC keys, being compact, resulted in reduced computing power requirements and minimized energy consumption. The study demonstrated that ECC proves to be a swift and efficient method for data protection in the context of cloud computing, contributing to lowered computing power demands and improved overall performance.

In the study outlined in [57], the authors introduced a novel lightweight encryption algorithm that involves a fusion of symmetric and asymmetric algorithms. This innovative combination enables users to enjoy the security advantages of asymmetric encryption and the swift performance of symmetric encryption, all while ensuring users' rights to protected and authorized access to data. The study demonstrated that the processing time of this lightweight algorithm is quicker compared to contemporary cryptographic algorithms.

The authors of the study [58] presented a system for cloud computing privacy-preserving outsourced classification (POCC). With the help of this framework, the evaluator can safely train a classification model on data that has been outsourced to numerous data providers and encrypted using different public keys. The authors used a proxy completely homomorphic encryption method, building on Gentry's system, to protect private information.

A framework that included a number of methods and specific steps to effectively safeguard data from the owner to the cloud and back to the user was presented in [59]. Data protection techniques included encoding the data, dividing it into three portions within the cloud, and using a secure socket layer (SSL) and MAC to guarantee data integrity. The partitioning of the data into three sections increases accessibility while simultaneously strengthening security. As data moves from the server owner to the cloud and from the cloud to the consumer, the suggested approach successfully achieves data availability, dependability, and integrity. It also gives users more freedom by allowing them to search for and retrieve encrypted data from the cloud.

The authors of [60] presented a brand-new method called match-then-decryption, which includes a matching stage prior to the decryption procedure. Without actually decrypting the ciphertexts, this technique computes certain parts of the ciphertexts to confirm if the private key attribute matches the hidden access policy in ciphertexts. By means of formal security studies and comparisons, it was shown that the suggested solutions may maintain privacy characteristics while improving decryption efficiency for cloud data storage that is outsourced.

The authors presented a secure cloud computing paradigm based on data classification in research published in [61]. The model uses TLS, AES, and SHA cryptographic methods that are specific to the type of classified data in order to reduce the total amount of time needed to secure the data. The outcomes of the testing showed how the suggested approach could be implemented effectively and with reliability.

The study in [62] provided a classification method based on multiple factors that were defined in multiple dimensions. The idea is to define security tiers based on accessibility and content type. The authors claim that data security can be customized based on the level of protection that is needed and that equivalent storage security measures can be implemented based on the size of the classified data collection.

In [63], a system was presented with the goal of improving the RSA algorithm by increasing the key size, which would fortify the encryption process. The suggested approach increases the algorithm's strength through larger key sizes while decreasing the time required for encryption and decryption by splitting the material into blocks. This enhancement makes cloud data storage more efficient.

The authors of the work in [64] provided a framework intended to protect massive data in cloud computing settings. The investigation determined how many people were gaining access to the cloud data center by using the MapReduce framework. The Meta cloud data storage interface was used by the suggested architecture to secure the mapping of various data elements to each provider. This method offers important insights for improving security in cloud computing environments, even though it requires a large implementation effort that can affect systems in the future.

In summary, the suggested solutions for safeguarding cloud data encompass diverse approaches, including data

auditing, encryption, classification, and secure data modeling. Nevertheless, these methodologies are not yet fully developed and encounter several challenges.

4.2. Solutions at the Application Level

Researchers have proposed a number of strategies to mitigate vulnerabilities at the application level. One study, described in [65], for example, presented a unique strategy called "Scale Inside Out," which aims to quickly absorb Distributed Denial of Service (DDoS) attacks and decrease the Resource Utilization Factor during attacks. Redistributing victim service resources and other co-located facilities to the prevention service for the purpose of assessing availability during the assault is the suggested option. The study's experimental evaluations show a significant 95% reduction in the overall attack downtime for the victim's service in addition to significant improvements in attack detection, reporting time, and co-located facility downtime.

Researchers provided a method to thwart EDoS assaults in an SDN-based cloud computing environment in a report published in [9]. As a multivariate time, series anomaly detection model, they used Long Short-Term Memory (LSTM), an unsupervised deep learning technique. Predicting a cloud customer's resource utilization, such as memory usage and CPU load, was the main notion. The researchers found that the suggested strategy for thwarting EDoS attacks in an SDN-based cloud was not only novel but also successful through tests carried out at different EDoS attack intensities.

A research project came out with a way to identify Distributed Denial of Service (DDoS) assaults in cloud computing in [66]. For classification, this approach makes use of machine learning methods such as Random Forest (RF), Naive Bayes (NB), and Support Vector Machine (SVM). A unique dataset designed exclusively for the intrusion detection method was produced as a result of the study's employment of Tor Hammer as an assault tool in a cloud setting.

A study contribution published in [67] offered a method to lessen the effects of economic denial of service (EDoS) assaults on cloud services. This strategy depends on putting in place an intrusion prevention system (IPS) in addition to a service level agreement (SLA).

The authors of [68] presented a novel multi-server authentication mechanism for mobile cloud computing (MCC) environments, based on elliptic curve cryptography (ECC). In addition to guaranteeing computational efficiency, this suggested technique preserves the features of pricey pairing schemes, such as scalability, anonymity, and safe mutual authentication. A formal security model provides a theoretical demonstration of the scheme's efficacy.

In another study [69], a unique method for identifying Economic Denial of Service (EDoS) attacks in the cloud was suggested. This method used an artificial neural network (ANN) in combination with a genetic algorithm (GA). In order to classify cloud server users and lessen denial-of-service (EDoS) attacks, an artificial neural network (ANN) was used in the classification process. In parallel, appropriate fitness functions were used to optimize server attributes using the GA.

Employing the OpenStack platform as a foundation, the researchers in [70] developed a number of models for information and resource sharing across tenants in an Infrastructure as a Service (IaaS) cloud. These models promote tenants to collaboratively utilize their IT resources in a regulated manner. However, it is essential to impose restrictions on Virtual Machines (VMs) regarding network access to prevent the uncontrolled transmission of information by malicious software.

In order to improve the security of cloud resources, a framework supporting passphrase-based multifactor authentication was presented in [71], where several authentication algorithms used in cloud computing were examined. The main assessment of authentication models focused on the security capabilities and limitations of the corresponding schemes in the context of cloud computing. The suggested method adds further protection to the SSH key pair and uses passphrases to guarantee safe passwords.

The author presented a novel access control architecture in [72] that addressed privacy and security issues in cloud environments. With access control mechanisms in place to mitigate the possibility of unwanted activity and guarantee that only authorized users have access to cloud resources, the framework was built around dynamic trustworthiness. The results showed that the system could recognize harmful activity, blocking unwanted access and boosting user confidence while improving cloud computing security overall.

The authors of [73] suggested an authentication-based AES and MD5 solution for data encryption to safeguard user login credentials and data via the cloud at the time of login.

A study in [74] introduced a dynamic access control methodology aimed at addressing the diverse security breaches observed in cloud environments. This approach aims to enhance the security of cloud-stored data by addressing the connections between the requester, the requested data, and the intended action on the data. Additionally, the study incorporated dynamic user considerations in the access control process. However, it's important to note that the results provided only represent an initial implementation of the proposed approach.

The researchers in [75], the researchers presented an innovative security model designed to enhance authentication in cloud computing through biometric support. This model introduced a novel concept incorporating fingerprint recognition for biometric security. The proposed method automated the verification process by comparing human fingerprints, utilizing them for individual identification and identity verification. Authentication of users relied on fingerprint templates generated from random numbers on each occasion. The experimental outcomes demonstrated the superior performance of the proposed system compared to a single-fingerprint authentication system.

Researchers presented a hybrid access control system called iHAC in this study [76]. It combines elements of role-based access control with type enforcement. This framework offers integrated, flexible access control for cloud settings that use Infrastructure as a Service (IaaS). Furthermore, an access control technique based on Virtual Machine Monitor (VMM) was created to precisely limit VM behaviors with respect to the underlying resources. According to experimental findings, the iHAC framework enables precise access control decisions with a manageable amount of performance overhead.

Researchers presented a novel multi-factor, hash-based, secure mutual authentication approach in [77], which included mathematical hashing properties, certificates, nonce values, conventional user IDs, and password mechanisms. Using the GNY belief logic and the Scyther approach, the robustness of the suggested authentication procedure was assessed. The results show how well the proposed strategy works to stop replay, man-in-the-middle, and forgery attacks.

A blockchain-based access control architecture called AuthPrivacyChain, which is aimed at protecting privacy in cloud environments, was presented in a recent paper [78]. Transaction authorization is verified by the user and entered onto the blockchain. The enterprise operation system (EOS) blockchain, which provides information and access permissions as well as extra details for blockchain transactions, is the foundation around which the framework is built. Access control, authorization revocation, and authorization are among the functions provided by AuthPrivacyChain. Only authorized users are able to access resources, according to experimental results, however AuthPrivacyChain is powerless to stop external user attacks.

In a recent study [79], a secure session for cloud-based mobile edge computing was established using a Seamless Secure Anonymous Authentication Scheme (S-SAAS). This protocol ensured smooth communication by using elliptic-curve cryptography, a one-way hash function, and economical operations. In order to prevent such attacks and still adhere to basic security standards, the protocol also included a unique random integer.

In a study project [80], a blockchain-based method for strengthening cloud identity management with better security and privacy was put forth. This method provides a decentralized trust and authentication mechanism. This trust framework, in contrast to previous models, establishes interactive trust relationships between clients and cloud service providers (CSPs) without the need for pre-configured parameters or rules. As a result, this strategy successfully maintains trust connections and guarantees safe Infrastructure as a Service (IaaS) for cloud federations, as evidenced by the favorable results concerning privacy and security capabilities.

Identity and access management (IAM) as a service, or IAMaaS, can be made available to the general public by Cloud Service Providers (CSPs) thanks to a methodology offered in the research described in [81]. The purpose of this framework is to guarantee that identity management adheres to cloud computing standards. The authors claim that IAMaaS enhances security capabilities by easily integrating in a hybrid approach with current on-premise technologies. Furthermore, IAMaaS gives customers the ability to create a virtual private area in the cloud, which strengthens security and protects their assets.

Using fuzzy cognitive maps, the researcher in [82] presented a ground-breaking dynamic trust model for Federated Identity Management (FIM). In order to improve the flexibility and scalability of FIM for deployment and maintenance in cloud environments, this concept sought to dynamically and safely assess trust relationships across new entities. Furthermore, the suggested model provided a collection of trust traits that served as the foundation for modeling and quantifying the degrees of trust connected to unknown entities.

In [83], the author reports that researchers devised an Identity Management System (IDMS) intended to maintain cloud computing communication security between servers and clients. In order to mitigate privacy breaches, the system used the Dual Certificate Manager (DCM) mechanism to authorize and authenticate users. The DCM approach reduced the attack surface by tracking and enabling data access using token-based language. Notably, the SSL/TLS protocol, which ensures secure data transmission, widely uses this technology.

In summary, the examination of literature solutions at the application level underscores a predominant focus on Intrusion Detection and Prevention Systems (IDS/IPS) for addressing DDoS and EDoS risks. Despite their utility, these techniques exhibit limitations, particularly in handling intricate and unknown attack patterns, necessitating more sophisticated approaches for detection and prevention in cloud environments. Moreover, problems with managing privileges and trust relationships, which are crucial for fending off both internal and external threats mean that traditional firewalls, encryption, and virtualized access control as well as other identity management and access control solutions, are considered inadequate for enhancing security. As a result, researchers are urged to integrate advanced technologies such as blockchain to enhance security measures.

4.3. Solutions at the Network Level

In a recent investigation documented in [10], a method was introduced for end-users to encrypt and distribute data blocks randomly within a Peer-to-Peer (P2P) network utilizing blockchain technology. The distributed cloud environment consists of multiple data centers and users, which can occasionally present challenges in determining the optimal placement of file block replicas. Consequently, the utilization of blockchain is considered an ideal approach to address concerns related to file security and network transmission delays.

The investigation outlined in [84] introduced various security measures employed to deter unauthorized access to cloud computing environments. These measures encompass certificates, including Public Key Infrastructure (PKI), robust authentication and authorization processes, and diverse encryption techniques, such as both symmetric and asymmetric key algorithms.

The researchers in [85] concentrated on identifying Distributed Denial of Service (DDoS) attacks through the creation of a deep learning classifier. Service requests from users were gathered and organized as log data. Using the Bhattacharya distance measure to reduce the classifier's training time, important characteristics from the log file were selected for classification. The simulation outcomes indicated that the proposed DBN classifier, based on TEHO, exhibited enhanced detection performance.

OpenPipe is a Software-as-a-Service (SaaS) concept developed by the research provided in [86]. With a software-defined network (SDN) controller at the top and local controllers at the bottom of the hierarchical tiers, this model adopted a hybrid control method. The SDN controller provided network virtualization and programmability by operating as a barrier between the control plane and the data plane. An efficacious demonstration of OpenPipe was carried out in a lab.

The researchers presented a Bayesian network-based method for building weighted attack path models in [87]. They also demonstrated an improved method that takes important nodes and edges into account while determining the shortest attack path among several sources. In addition to finding the shortest path, this technique breaks ties between pathways that have equal weights.

Hypervisor Level Distributed Network Security (HLDNS) is a framework that was proposed by the work in [88] and should be installed on every cloud server. In order to detect intrusions, each server is in charge of keeping an eye on network activity between virtual machines (VMs) and other components, including the internal, external, and virtual networks. Using recent intrusion detection datasets like UNSW-NB15 and CICIDS-2017, real-time experiments mimicking various attacks at NIT Goa were used to assess the efficacy of the HLDNS system, with good findings.

A novel dynamic proof of communication-efficient recovery was introduced in the research described in [89], supporting public audibility in the event of data corruption through schemes for irretrievability. Both the coding operation and the data blocks, which were carried out separately for each block, made up the partitioned data. Designed to minimize the impact of updates on remote data, this strategy is appropriate for storage and guarantees that updates will only influence minor codeword symbols. An efficient data reform plan for server failure scenarios was also suggested by the study.

In order to prevent Distributed Denial of Service (DDoS) and Denial of Service (DoS) assaults in cloud computing, the researchers proposed using SNORT as an intrusion detection system in [90]. DDoS attacks force the server to become unavailable to authorized users by flooding it with an excessive number of pointless packets. To detect and stop DDoS attacks, the suggested solution makes use of pre-established rules.

In a similar manner, [91] presented a method for identifying and classifying different DDoS assaults in cloud computing settings. This approach combines an artificial neural network (ANN) with the GARCH model. In real traffic, GARCH is used to estimate variances and spot possible anomalies, whereas ANN filters out values below a predetermined threshold and then makes the distinction between normal and abnormal traffic.

In [92], the researchers provided an overview of various attacks targeting the DNS infrastructure. They highlighted the prevalent use of firewalls as a key defense mechanism in configuring DNS servers effectively. Additionally, the deployment of dynamic DNS firewalls, along with suitable signatures, was emphasized as a protective measure against a wide range of potential attack vectors.

At this level, greater focus was placed on mitigating DoS/DDoS attacks through the use of IDS/IPS techniques. However, these methods exhibit inaccuracies, generating false alarms for legitimate requests, and are effective only against specific or individual attacks. Moreover, these solutions do not effectively address IP spoofing, a tactic frequently employed by attackers in DoS/DDoS scenarios to overwhelm networks. Consequently, they struggle to distinguish between legitimate and malicious traffic. Additionally, minimal efforts have been directed toward countering prefix hijacking attacks, a significant concern.

It's noteworthy that more attention has been directed towards ensuring network availability by addressing DNS issues through firewalls. However, conventional firewalls are still unable to stop several types of DNS assaults, such as man-in-the-middle attacks, changed data attacks, DNS ID spoofing attacks, corrupted data attacks, and distributed denial-of-service attacks. These challenges necessitate the exploration of alternative techniques.

4.4. Solutions at the Host Level

A preventive strategy was developed by the researchers in [93] to counter DDOS assaults in hypervisor systems. This framework operated on an intrusion detection defense system that was host-based and specifically built on intrusion detection modeling. After then, it was included with IPS in the hypervisor environment. The prevention model utilized principal component analysis and linear discriminant analysis for the identification and design of the cloud server. In addition, a hybrid metaheuristic technique called Ant Lion optimization was utilized for feature selection, which was inspired by nature. The next step was to use a classifier, which was an artificial neural network. The results showed that the model was successful in identifying malicious activity and blocking it by blocking the offending IP address on the blacklist.

The researchers presented a novel method in [94] that combined an intrusion detection system, prevention system, and virtual machine that could operate both inside and outside of a box. Finding vulnerabilities was the main goal, which included enduring threats such as denial-of-service attacks and covert self-concealing rootkits. The Open-Source Security Event Correlator (OSSEC), an open-source host that served as an IDS, was used in the experiment. The trials' outcomes demonstrated how well OSSEC IDS works to identify rootkits and denial-of-service attacks on Linux and

Windows platforms.

Hypervisor Intrusion Detection System (VMHIDS), which is intended to detect and prevent hypervisor intrusions, was investigated in [95] for its effectiveness as a preventative measure in virtualized cloud environments. Comprehensive protection against possible internal or external attacks within the cloud environment was offered by this technology for both the hypervisor and virtual machines. Using real-time event analysis made possible by VMHIDS's continuous hypervisor and virtual machine monitoring, malicious activity could be automatically detected and stopped. In order to guarantee quick detection and defense against any new or suspected assaults on hypervisors, the system kept a close eye on every file and process that interacted with it.

By implementing virtual machine security policies, a suggested system in [96] aimed to minimize co-located VM assaults within the same hypervisor. The framework was specifically created to detect and handle instances of live virtual machines (VMs) being copied or transferred without authorization to an untrustworthy hypervisor. In order to identify irregularities at particular times, the implementation involved tracking the data traffic rates between two virtual machines (VMs) and the VSwitch node. Results from the study demonstrated that the framework effectively reduced the associated risks related to VMs running on the identified suspicious hypervisor. It's worth noting that this framework was tailored to address live migration scenarios involving individual VMs.

In [97], the study delved into virtualization challenges within cloud computing infrastructure. It recognized distributed side-channel attacks as one of the main dangers that could be used to steal confidential data from different parts of a distributed system. The research suggested using an autonomic system as a means of countering these side-channel attacks.

Meanwhile, in [98], researchers recommended a framework employing VM monitoring scripts to safeguard VMs from potential attacks. This required adding a smart virtualization monitoring system to the virtual machine manager (KVM) that runs on the kernel. By actively collecting status data from every virtual machine (VM) operating under a hypervisor, the approach made it possible to categorize and proactively fix attack patterns. The framework communicated the necessary corrective actions through the cloud API.

A cloud-based security-as-a-service model that functions at the host level was proposed in [99]. The purpose of this model is to alert the host to any harmful activity taking place on the system. In addition, the system call traces were classified using a K-nearest neighbors (KNN) classifier, which made it easier to add additional training data. The results showed that the recommended strategy achieved a noteworthy degree of detection accuracy.

In [100], an assessment was conducted on the efficacy of Ceilometer and Monasca, private cloud infrastructure tools, to rapidly detect resource constraints and assess the impact of resource utilization on host systems. The evaluation demonstrated that Monasca outperformed Ceilometer in terms of performance.

In the meantime, [101] put into practice signature-based network intrusion detection systems (NIDS), combining SNORT for intrusion detection at the network and cloud virtual machine (VM) levels with OSSEC as a host-based IDS. The study looked at monitoring and traffic flow in a variety of settings. The results showed that the suggested solutions were successful in detecting host virtual machine threats and notifying the organization of them.

The Security-aware Virtual Machine Placement Algorithm (SMOOP) was presented by the researchers in [101]. It employs a multi-objective optimization technique to determine a Pareto-optimal approach for reducing overall security risks in the cloud. SMOOP assessed cloud security by taking a location-specific and multidimensional approach to networking, co-residence, virtual machine, and hypervisor vulnerabilities. The outcomes of the trial proved how beneficial and effective the suggested strategy was in comparison to other options.

Additionally, [102] introduced the online non-clairvoyant scheduling technique known as Highest Scaled Importance First (HSIF). To reduce the total of scaled importance-based flow time and energy consumption, HSIF chooses the most important active work. The use of HSIF in battery-powered devices and data centers lowers power consumption while increasing computational capacity.

In [103], an energy-efficient task-scheduling algorithm based on the best-worst (BWM) and the technique for order preference by resemblance to the ideal solution (TOPSIS) was proposed in order to assess the significance of various cloud scheduling solutions. Comparing the suggested strategy to other approaches, experimental findings show that it successfully lowers energy use. The method also considerably increases virtual machine (VM) use, which makes it a good fit for solving complex issues.

According to [104], extensive data centers can reduce their energy consumption without sacrificing the overall performance of cloud computing systems by implementing a parameterized scheduling strategy that minimizes the makespan in conjunction with an energy-efficient policy that bases each virtual machine's hibernation whenever possible. The authors of the same paper presented a model that aims to reduce energy consumption in cloud computing environments, showing that a cloud computing system's energy usage can be reduced by up to 45%. An energy-aware independent batch scheduler and a collection of energy-efficient idle virtual machine (VM) hibernation strategies make up the model. The experimental results demonstrate how well the suggested model works.

Additionally, the SCORE tool was presented in this study [105] as an addition to the Google Omega lightweight simulator. With the purpose of simulating energy-efficient parallel and monolithic scheduling methods, SCORE is specifically made to support the execution of synthetic, realistic, and heterogeneous workloads. Based on practical evaluations, the simulator was found to be a reliable and effective tool for evaluating scheduling techniques, security, and energy efficiency in cloud computing environments.

In summary, when devising detection or prevention techniques, it is imperative for proposed solutions to address

formidable threats such as distributed side-channel attacks, which may seriously harm cloud infrastructures by taking advantage of private information that is dispersed among different distributed system components [98]. Host-level techniques, though valuable, still require further development to ensure swift responses, automatic blocking of malicious events, and the implementation of appropriate actions to preemptively thwart potential attacks from occurring.

Table 3. Summary of the literature's current solutions

Level Name	Techniques	Limitations	References
Data Level	Data is protected from loss or unauthorized disclosure through the use of encryption technologies like TLS, AES, and SHA. Classification techniques are often applied to determine data security levels.	Encryption methods are not yet fully developed and encounter various challenges. The current classification technique demands significant resource consumption.	[52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 67, 106]
Application Level	Distributed Denial of Service (DDoS) assaults on cloud applications and services were countered using Intrusion Detection and Prevention Systems (IDS/IPS) techniques. IDS/IPS methods were implemented to mitigate Economic Denial of Service (EDoS) attacks. To address issues related to weak authentication, AES and MD5-based authentication methods as well as Identity Management Systems (IDMS) were among the solutions.	Current methods primarily address straightforward DDoS attacks, yet the dynamic nature of cloud environments necessitates techniques capable of preventing and detecting intricate attacks with unfamiliar patterns. The methods employed to address simple attacks. Testing in constrained environments and employing limited datasets are regarded as obstacles to implementation. Traditional access control and identity management measures may not be conducive to enhancing security.	[10, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 107]
Network Level	The existing techniques for dealing with Denial of Service (DoS) and Distributed Denial of Service (DDoS) assaults entail using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Various techniques address DNS issues, ranging from dynamic firewalls to intrusion detection systems (IDS).	Certain DDoS/DoS techniques do not effectively handle IP spoofing, a method frequently employed in these attacks to overwhelm networks. As a result, distinguishing between legitimate and malicious traffic becomes challenging. These approaches overlooked significant threats, includes attacks that manipulate data, spoof DNS IDs, corrupt data, and man-in-the-middle.	[11, 84, 85, 86, 87, 88, 89, 90, 91, 92]
Host Level	Virtual machine monitoring and intrusion detection are the techniques used to handle issues with virtual machines and hypervisors.	These approaches restricted their methods to particular scenarios, familiar attack patterns, or specific software. While developing detection or prevention approaches, there is a need to provide more attention to addressing various forms of assaults, such as distributed side-channel attacks.	[12, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105]

5. Future Recommendations and Research Opportunities

5.1. Future Recommendations

Various solutions must be incorporated into a holistic approach to address the security challenges in cloud computing. The following are some crucial tactics to improve cloud security:

Effective Identity and Access Management (IAM)

Only authorized users can access particular resources by using IAM platforms with strong controls, such as multi-factor authentication, least-privilege access, and strict password policies. It could be necessary for remote workers to use Virtual Private Networks (VPNs) in order to access critical resources over public Wi-Fi.

Data Security and Loss Prevention

Sensitive data can be encrypted, access and usage can be tracked, and suspicious activity can be alerted to through the use of Data Loss Prevention (DLP) technologies and a comprehensive data security platform. To reduce harm in the event of a breach, regular data backups are essential.

Firewall Protection

Firewalls play a crucial role in preventing threat actors from infiltrating the network. They can block malicious traffic both entering and leaving the network, including attempts by malware to communicate with command and control servers.

Security Awareness Training

Conducting security awareness training helps users identify and avoid common cyberattack vectors, including phishing and social engineering attacks.

Vulnerability Management

Implementing vulnerability management policies, which include scheduled patch management and regular penetration testing, helps identify and address vulnerabilities before they can be exploited by hackers.

Attack Surface Management (ASM)

Utilizing ASM tools can identify, catalog, and remediate potentially vulnerable assets, proactively addressing security risks before they are exploited by cyberattacks.

Unified Endpoint Management (UEM)

UEM tools enforce security policies and controls across all endpoints on the corporate network, covering laptops, desktops, and mobile devices.

Robust Authentication and Access Controls

To ensure that only authorized users may access cloud resources, implement robust authentication methods like multi-factor authentication (MFA) and strict access controls.

Data Encryption

To protect sensitive data, even in the case of illegal access, make use of strong encryption techniques and handle encryption keys safely.

Regular Security Updates and Patching

To fix known vulnerabilities, keep all cloud environment components such as operating systems, apps, and virtual machines—up to date with the most recent security patches and upgrades.

Network Segmentation and Firewalls

Segment your network to isolate important resources, and use firewalls to control incoming and outgoing traffic so that only authorized communication is permitted.

Security Monitoring and Logging

Deploy comprehensive security monitoring tools to promptly detect and respond to security events and anomalies, ensuring a proactive security posture.

Vendor Due Diligence

Perform comprehensive evaluations of cloud service providers, analyzing their certifications, security protocols, and adherence to pertinent standards to ensure that they meet organizational needs.

Employee Training and Awareness

Emphasize adherence to security rules and procedures, educate staff members on cloud security best practices, and increase their understanding of the dangers of phishing and data breaches.

Incident Response Planning

To guarantee a prompt and efficient response to security issues, create and test an incident response plan that outlines roles, responsibilities, escalation procedures, and communication channels.

Continuous Security Assessments

To find and fix flaws or vulnerabilities in the cloud environment, do routine security assessments, such as penetration testing and vulnerability scanning.

Compliance and Regulatory Adherence

In order to satisfy legal and regulatory obligations, make sure that industry standards and regulations—like the CCPA, CPRA, GDPR, and others are followed.

Third-Party Risk Management

Evaluate and control the risks connected to outside partners or vendors having access to the cloud environment. To protect data, put contractual agreements and security measures in place.

5.2. Future Research Opportunities

Absolutely, the dynamic evolution of the cloud computing landscape opens up numerous promising directions for future research, encompassing technological advancements as well as the resolution of non-technical challenges. Below are potential areas for future research in the field of cloud computing:

Security and Privacy Enhancements

- Develop more robust encryption techniques and privacy-preserving mechanisms to ensure data security in multi-tenant cloud environments.
- Investigate the impact of emerging technologies like homomorphic encryption and zero-trust architectures on cloud security.

Edge and Fog Computing Integration

- Explore ways to seamlessly integrate edge and fog computing with cloud infrastructure to enhance performance, reduce latency, and improve the overall user experience.
- Investigate resource management and allocation strategies for distributed computing across cloud and edge/fog nodes.

Quantum Computing in Cloud

- Explore the implications of integrating quantum computing resources into cloud environments, considering both the potential benefits and security challenges.
- Investigate quantum-safe cryptographic algorithms to ensure data protection in a post-quantum computing era.

Energy Efficiency and Sustainability

- Develop energy-efficient algorithms and resource management strategies to minimize the environmental impact of large-scale cloud data centers.
- Explore the integration of renewable energy sources and green computing practices to make cloud infrastructure more sustainable.

Ethical and Legal Considerations

- Investigate the ethical implications of cloud computing, especially regarding data ownership, consent, and responsible AI usage.
- Examine legal frameworks and regulations related to cross-border data flow, data sovereignty, and jurisdictional issues in the cloud.

Hybrid and Multi-Cloud Architectures

- Study effective strategies for managing and orchestrating hybrid and multi-cloud environments, addressing challenges related to interoperability, data consistency, and workload portability.
- Explore new models for cloud federation and collaboration to enable seamless resource sharing across diverse cloud providers.

AI and Machine Learning in Cloud

- Investigate the integration of AI and machine learning services in cloud platforms, focusing on optimizing model training and deployment.
- Explore privacy-preserving techniques for federated learning in a cloud-based environment.

User Experience and Human-Computer Interaction

- Research ways to enhance the user experience in cloud applications, considering aspects such as interface design, accessibility, and user-centric performance optimization.
- Examine the impact of cloud computing on user behavior and productivity in various domains.

Blockchain and Distributed Ledger Technologies

- Explore the integration of blockchain and distributed ledger technologies to enhance the transparency, integrity, and accountability of cloud-based systems.
- Investigate the potential use of blockchain for secure and auditable cloud transactions.

Business Models and Economics of Cloud Computing

- Examine the economic implications of different cloud service models and deployment options for businesses.
- Investigate novel business models, pricing strategies, and cost optimization techniques in the cloud.

These research opportunities reflect the interdisciplinary nature of cloud computing, encompassing technical innovation, security, ethics, sustainability, and user-centric considerations. Future research in these areas can contribute to the continuous evolution and improvement of cloud infrastructure.

6. Conclusions

The alluring attributes of cloud computing, including its flexibility, cost-effectiveness, utility, and potential for savings, make it a cutting-edge and highly appealing technology. Despite its numerous benefits, the adoption of cloud computing is hindered by substantial security and privacy concerns. Recognizing that security awareness is a crucial initial step in promoting cloud adoption, users and organizations engaging with cloud services need to be knowledgeable about potential threats, attacks, and vulnerabilities. The problems and difficulties with the cloud computing infrastructure were covered in this study at several levels (Application, Network, Host, Data). Numerous pre-existing methods were presented to address these issues and mitigate them. However, because of the shared, virtualized, dispersed, and open nature of the cloud, many holes remain unfilled, and new issues keep coming up. This article then concentrated on alternative approaches to handle security concerns in the cloud infrastructure at various layers.

References

[1] Elsherbiny, S.; Eldaydamony, E.; Alrahmawy, M.; Reyad, A.E. An extended Intelligent Water Drops algorithm for workflow scheduling in cloud computing environment. Egypt. Inf. J. 2018, 19, 33–55.

[2] Hanen, J.; Kechaou, Z.; Ben Ayed, M. An enhanced healthcare system in mobile cloud computing environment. Vietnam J. Comput. Sci. 2016, 3, 267–277.

[3] Bassi, Sonia, and Anjali Chaudhary. "Cloud Computing Data Security–Background and Benefits." International Journal of Computer Science & Communication 6.1 (2015).

[4] On technical security issues in cloud computing, Meiko Jensen etal, 2009.

[5] Mell, P.; Grance, T. The NIST Definition of Cloud Computing; Nation-al Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.

[6] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud definition, in:ACM SIGCOMM Computer Communication Review, 2008.p.50-55.

[7] M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6.

[8] Hatwar, S.V.; Chavan, R. Cloud Computing Security Aspects, Vulnerabilities and Countermeasures. Int. J. Comput. Appl. 2015, 119, 46–53.

[9] Dinh, P.T.; Park, M. Dynamic Economic-Denial-of-Sustainability (EDoS) Detection in SDN-based Cloud. In Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 20–23 April 2020.

[10] Karajeh, H.; Maqableh, M.; Masa'deh, R. Privacy and security issues of cloud computing environment. In Proceedings of the 23rd IBIMA Conference Vision, Valencia, Spain, 13–14 May 2020.

[11] Han, J.; Zang, W.; Chen, S.; Yu, M. Reducing Security Risks of Clouds Through Virtual Machine Placement. In Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, Philadelphia, PA, USA, 19–21 July 2017.

[12] Saravanan, N.; Umamakeswari, A. Lattice based access control for protecting user data in cloud environments with hybrid security. Comput. Secur. 2021, 100, 102074.

[13] Zulifqar, I., Anayat, S. and Kharal, I., 2021. A Review of Data Security Challenges and their Solutions in Cloud Computing. International Journal of Information Engineering & Electronic Business, 13(3).

[14] Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M.A. and Al-Rimy, B.A.S., 2021. Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. Applied Sciences, 11(19), p.9005.

[15] Siddiqui, S.; Darbari, M.; Yagyasen, D. A Comprehensive Study of Challenges and Issues in Cloud Computing. In Soft Computing and Signal Processing; Springer: Singapore, 2019; pp. 325–344.

[16] Marston, S.; Li, Z.; Bandyopadhyay, S.; Ghalsasi, A. Cloud Computing—The Business Perspective. Decis. Support Syst. 2011, 51, 176–189.

[17] https://www.geeksforgeeks.org/cloud-stakeholders-as-per-nist/, accessed on 12/31/2023.

[18] Kuyoro, S.; Ibikunle, F.; Awodele, O. Cloud computing security issues and challenges. Int. J. Comput. Netw. 2011, 3, 247–255.

[19] Alajmi, Q.; Sadiq, A.S.; Kamaludin, A.; A Al-Sharafi, M. Cloud Computing Delivery and Delivery Models: Opportunity and Challenges. Adv. Sci. Lett. 2018, 24, 4040–4044.

[20] Diaby, T. and Rad, B.B., 2017. Cloud computing: a review of the concepts and deployment models. International Journal of Information Technology and Computer Science, 9(6), pp.50-58.

[21] Chauhan, V.K.; Bansal, K.; Alappanavar, P. Exposing cloud computing as a failure. Int. J. Eng. Sci. Technol. 2012, 4, 1320–1326.

[22] Faheem, M.; Akram, U.; Khan, I.; Naqeeb, S.; Shahzad, A.; Ullah, A.; Mushtaq, M.F. Cloud Computing Environment and Security Challenges: A Review. Int. J. Adv. Comput. Sci. Appl. 2017, 8, 183–195.

[23] Sikeridis, D., Papapanagiotou, I., Rimal, B.P. and Devetsikiotis, M., 2017. A Comparative taxonomy and survey of public cloud infrastructure vendors. arXiv preprint arXiv:1710.01476.

[24] 21. Subramanian, N.; Jeyaraj, A. Recent security challenges in cloud computing. Comput. Electr. Eng. 2018, 71, 28–42.

[25] Kumar, P.R., Raj, P.H. and Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, pp.691-697.

[26] Bokhari, M.U.; Makki, Q.; Tamandani, Y.K. A Survey on Cloud Computing. In Big Data Analytics; Advances in Intelligent Systems and Computing; Springer: Singapore, 2018; Volume 654, pp. 149–164.

[27] Abdurachman, E.; Gaol, F.L.; Soewito, B. Survey on Threats and Risks in the Cloud Computing Environment. Procedia Comput. Sci. 2019, 161, 1325–1332.

[28] Dong, S., Abbas, K. and Jain, R., 2019. A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, pp.80813-80828.

[29] Alhenaki, L., Alwatban, A., Alamri, B. and Alarifi, N., 2019, May. A survey on the security of cloud computing. In 2019 2nd international conference on computer applications & information security (ICCAIS) (pp. 1-7). IEEE.
[30] Tabrizchi, H.; Rafsanjani, M.K. A survey on security challenges in cloud computing: Issues, threats, and solutions. J. Supercomput. 2020, 76, 9493–9532.
[31] Domingo-Ferrer, J.; Farràs, O.; Ribes-González, J.; Sánchez, D. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Comput. Commun. 2019, 140, 38–60.
[32] Kumar, R. and Goyal, R., 2019. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, pp.1-48.
[33] Ibrahim, F.A.M.; Hemayed, E.E. Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review. Comput. Secur. 2019, 82, 196–226.
[34] Qureshi, A.; Dashti, W.; Jahangeer, A.; Zafar, A. Security Challenges over Cloud Environment from Service Provider Prospective. Cloud Comput. Data Sci. 2020, 1, 1–48.
[35] An, Y.Z.; Zaaba, Z.F.; Samsudin, N.F. Reviews on Security Issues and Challenges in Cloud Computing. IOP Conf. Ser. Mater. Sci. Eng. 2016, 160, 012106.
[36] Saini, H.; Saini, A. Security Mechanisms at different Levels in Cloud Infrastructure. Int. J. Comput. Appl. 2014, 108, 1–6.
[37] Cloud computing: security risks and security measures, Ben Nancholas, https://online.york.ac.uk/cloud-computing-security-risks-and-security-measures/, accessed on 2/1/2024.
[38] Harpreet Saini, Amandeep Saini, "Security Mechanisms at different Levels in Cloud Infrastructure", International Journal of Computer Applications. Volume 108 – No. 2, December 2014. http://dx.doi.org/10.5120/18880-0153.
[39] Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems. Vol. 28, Issue 3, March 2012, Pages 583–592 http://dx.doi.org/10.1016/j.future.2010.12.006
[40] Vahid Ashktorab, Seyed Reza Taghizadeh, "Security Threats and Countermeasures in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM). Volume 1, Issue 2, October 2012,
[41] R. Charanya, M.Aramudhan, K. Mohan, S. Nithya, "Levels of Security Issues in Cloud Computing", International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr-May 2013
[42] Katerina Lourida1, Antonis Mouhtaropoulos2, Alex Vakaloudis3, "Assessing Database and Network Threats in Traditional and Cloud Computing", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(3): 1-17, 2013
[43] Aarti Singh, Manisha Malhotra, "Security Concerns at Various Levels of Cloud Computing Paradigm: A Review", International Journal of Computer Networks and Applications. Vol. 2, Issue 2, March – April (2015).
[44] Kashif Munir and Sellapan Palaniappan, "Security Threats/Attacks Present in Cloud Environment", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.12, December 2012.
[45] Kashif Munir and Prof Dr. Sellapan Palaniappan, "secure cloud architecture", Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, January 2013
[46] Jaydip Sen, "Security and Privacy Issues in Cloud Computing", Chapter 1. Architectures and Protocols for Secure Information Technology Infrastructures. IGI Global. Pp. 1-45. DOI: 10.4018/978-1-4666-4514-1.ch001
[47] Ankur Pandey,Kirtee Shevade, Roopali Soni , "Application Level Security in Cloud Computing", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012,5369-5373
[48] Tauseef Ahmad, Mohammad Amanul Haque, Khaled Al-Nafjan, Asrar Ahmad Ansari, "Development of Cloud Computing and Security Issues", Information and Knowledge Management. Vol.3, No.1, 2013.
[49] Top 10 Security Issues in Cloud Computing, https://www.veritis.com/blog/top-10-security-issues-in-cloud-computing/, accessed on 2/1/2024.
[50] Zero-Day-Exploits & Zero-day Attack, https://www.kaspersky.com/resource-center/definitions/zero-day-exploit, accessed on 3/1/2024.
[51] What are insider threats? https://www.ibm.com/topics/insider-threats, accessed on 3/1/2024.
[52] Singh, A.P.; Pasupuleti, S.K. Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing. Procedia Comput. Sci. 2016, 93, 751–759.
[53] Balogh, Z.; Turˇcáni, M. Modeling of data security in cloud computing. In Proceedings of the 2016 Annual IEEE Systems Conference (SysCon), Orlando, FL, USA, 18–21 April 2016.
[54] Vurukonda, N.; Rao, B.T. A Study on Data Storage Security Issues in Cloud Computing. Procedia Comput. Sci. 2016, 92, 128–135.
[55] Sajay, K.R., Babu, S.S. and Vijayalakshmi, Y., 2019. Enhancing the security of cloud data using hybrid encryption algorithm. Journal of Ambient Intelligence and Humanized Computing, pp.1-10.
[56] Khan, I.A.; Qazi, R. Data Security in Cloud Computing Using Elliptic Curve Cryptography. Int. J. Comput. Commun. Netw. 2019, 1, 46–52.
[57] Belguith, S.; Jemai, A.; Attia, R. Enhancing data security in cloud computing using a lightweight cryptographic algorithm. In Proceedings of the Eleventh International Conference on Autonomic and Autonomous Systems, Rome, Italy, 24–29 May 2015.
[58] Li, P., Li, J., Huang, Z., Gao, C.Z., Chen, W.B. and Chen, K., 2018. Privacy-preserving outsourced classification in cloud computing. Cluster Computing, 21, pp.277-286.
[59] Sood, S.K. A combined approach to ensure data security in cloud computing. J. Netw. Comput. Appl. 2012, 35, 1831–1838.
[60] Zhang, Y.; Chen, X.; Li, J.; Wong, D.S.; Li, H.; You, I. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Inf. Sci. 2017, 379, 42–61.
[61] Tawalbeh, L.; Darwazeh, N.S.; Al-Qassas, R.S.; AlDosari, F. A Secure Cloud Computing Model based on Data Classification. Procedia Comput. Sci. 2015, 52, 1153–1158.
[62] Shaikh, R.; Sasikumar, M. Data Classification for Achieving Security in Cloud Computing. Procedia Comput. Sci. 2015, 45, 493–498.
[63] Amalarethinam, I.G. and Leena, H.M., 2017, February. Enhanced RSA algorithm with varying key sizes for data security in cloud. In 2017 World Congress on Computing and Communication Technologies (WCCCT) (pp. 172-175). IEEE.
[64] Manogaran, G.; Thota, C.; Kumar, M.V. MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing. Procedia Comput. Sci. 2016, 87, 128–133.

[65] Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Rajarajan, M. Scale Inside-Out: Rapid Mitigation of Cloud DDoS Attacks. IEEE Trans. Dependable Secur. Comput. 2018, 15, 959–973.
[66] Wani, A.R.; Rana, Q.P.; Saxena, U.; Pandey, N. Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019.
[67] Ficco, M.; Rak, M. Economic denial of sustainability mitigation in cloud computing. In Organizational Innovation and Change; Springer International Publishing: Cham, Switzerland, 2016; pp. 229–238.
[68] Irshad, A., Chaudhry, S.A., Alomari, O.A., Yahya, K. and Kumar, N., 2020. A novel pairing-free lightweight authentication protocol for mobile cloud computing framework. IEEE Systems Journal, 15(3), pp.3664-3672.
[69] Nautiyal, S.; Wadhwa, S. A Comparative Approach to Mitigate Economic Denial of Sustainability (EDoS) in a Cloud Environment. In Proceedings of the 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019.
[70] Zhang, Y.; Krishnan, R.; Sandhu, R. Secure Information and Resource Sharing in Cloud Infrastructure as a Service. In Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, Scottsdale, AZ, USA, 3 November 2014; pp. 81–90.
[71] Rehman, F.; Akram, S.; Shah, M.A. The framework for efficient passphrase-based multifactor authentication in cloud computing. In Proceedings of the 2016 22nd International Conference on Automation and Computing (ICAC), Colchester, UK, 7–8 September 2016.
[72] Banyal, R.K.; Jain, V.K.; Jain, P. Dynamic Trust Based Access Control Framework for Securing Multi-Cloud Environment. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies— ICTCS '14, Udaipur, India, 14–16 November 2014.
[73] Ojha, S.; Rajput, V. AES and MD5 based secure authentication in cloud computing. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017.
[74] Auxilia, M.; Raja, K. Dynamic Access Control Model for Cloud Computing. In Proceedings of the 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, 17–19 December 2014.
[75] Rajeswari, P., Viswanadha Raju, S., Ashour, A.S. and Dey, N., 2017. Multi-fingerprint unimodel-based biometric authentication supporting cloud computing. Intelligent techniques in signal processing for multimedia security, pp.469-485.
[76] Zhou, C. and Li, B., 2014, December. iHAC: a hybrid access control framework for IaaS clouds. In 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing (pp. 853-858). IEEE.
[77] Lingamgunta, S., 2020. Multi Factor Two-way Hash-Based Authentication in Cloud Computing. International Journal of Cloud Applications & Computing, 10(2).
[78] Yang, C.; Tan, L.; Shi, N.; Xu, B.; Cao, Y.; Yu, K. AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. IEEE Access 2020, 8, 70604–70615.
[79] Deebak, B.D., Al-Turjman, F. and Mostarda, L., 2020. Seamless secure anonymous authentication for cloud-based mobile edge computing. Computers & Electrical Engineering, 87, p.106782.
[80] Bendiab, K., Kolokotronis, N., Shiaeles, S. and Boucherkha, S., 2018, August. WiP: A novel blockchain-based trust model for cloud identity management. In 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 724-729). IEEE.
[81] Sharma, D.H.; Dhote, C.; Potey, M. Identity and Access Management as Security-as-a-Service from Clouds. Procedia Comput. Sci. 2016, 79, 170–174.
[82] Bendiab, G.; Shiaeles, S.; Boucherkha, S.; Ghita, B. FCMDT: A novel fuzzy cognitive maps dynamic trust model for cloud federated identity management. Comput. Secur. 2019, 86, 270–290.
[83] Khajehei, K., 2018. Preserving Privacy in Cloud Identity Management Systems Using DCM (Dual Certificate Management). Int. J. Wirel. Microw. Technol, 8(4), pp.54-65.
[84] Maithili, K.; Vinothkumar, V.; Latha, P. Analyzing the Security Mechanisms to Prevent Unauthorized Access in Cloud and Network Security. J. Comput. Nanosci. 2018, 15, 2059–2063.
[85] Velliangiri, S.; Karthikeyan, P.; Kumar, V.V. Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. J. Exp. Artif. Intell. 2021, 1–20.
[86] Liang, K., Zhao, L., Chu, X. and Chen, H.H., 2017. An integrated architecture for software defined and virtualized radio access networks with fog computing. *IEEE Network*, *31*(1), pp.80-87.
[87] Zimba, A.; Chen, H.; Wang, Z. Bayesian network based weighted APT attack paths modeling in cloud computing. Future Gener. Comput. Syst. 2019, 96, 525–537.
[88] Patil, R., Dudeja, H. and Modi, C., 2019. Designing an efficient security framework for detecting intrusions in virtual network of cloud computing. *Computers & Security*, *85*, pp.402-422.
[89] Jouini, M.; Rabai, L.B.A. A. A security framework for secure cloud computing environments. In Cloud Security: Concepts, Methodologies, Tools, and Applications; IGI Global: Hershey, PA, USA, 2019; pp. 249–263.
[90] Hassan, Z., Odarchenko, R., Gnatyuk, S., Zaman, A. and Shah, M., 2018, October. Detection of distributed denial of service attacks using snort rules in cloud computing & remote control systems. In *2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)* (pp. 283-288). IEEE.
[91] Badve, O.P.; Gupta, B.; Yamaguchi, S.; Gou, Z. DDoS detection and filtering technique in cloud environment using GARCH model. In Proceedings of the 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 27–30 October 2015.
[92] Rajendran, B. and Shetty, P., 2018. Domain name system (dns) security: Attacks identification and protection methods. In *Proceedings of the International Conference on Security and Management (SAM)* (pp. 27-33). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
[93] Jaber, A.N.; Zolkipli, M.F.; Shakir, H.A.; Jassim, M.R. Host based intrusion detection and prevention model against DDoS attack in cloud computing. In Proceedings of the International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Barcelona, Spain, 8–10 November 2017.

[94] Kumara, A.; Jaidhar, C. Hypervisor and virtual machine dependent Intrusion Detection and Prevention System for virtualized cloud environment. In Proceedings of the 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), Kuala Lumpur, Malaysia, 26–28 May 2015.
[95] Dildar, M.S., Khan, N., Abdullah, J.B. and Khan, A.S., 2017, March. Effective way to defend the hypervisor attacks in cloud computing. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 154-159). IEEE.
[96] Ramamoorthy, S.; Rajalakshmi, S. A Preventive Method for Host Level Security in Cloud Infrastructure. In Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC–16'); Springer: Cham, Switzerland, 2016; pp. 3–12.
[97] Bazm, M.-M.; Lacoste, M.; Südholt, M.; Menaud, J.-M. Isolation in cloud computing infrastructures: New security challenges. Ann. Telecommun. 2019, 74, 197–209.
[98] Deshpande, S.M.; Ainapure, B. An Intelligent Virtual Machine Monitoring System Using KVM for Reliable And Secure Environment in Cloud. In Proceedings of the 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), Pune, India, 2–3 December 2016.
[99] Deshpande, P.; Sharma, S.C.; Peddoju, S.K.; Junaid, S. HIDS: A host based intrusion detection system for cloud computing environment. Int. J. Syst. Assur. Eng. Manag. 2018, 9, 567–576.
[100] Gomez-Rodriguez, M.A.; Sosa-Sosa, V.J.; Gonzalez-Compean, J.L. Assessment of Private Cloud Infrastructure Monitoring Tools. In Proceedings of the 6th International Conference on Data Science, Technology and Applications, Madrid, Spain, 26–28 July 2017.
[101] Mahajan, V. and Peddoju, S.K., 2017, August. Deployment of intrusion detection system in cloud: A performance-based study. In *2017 IEEE Trustcom/BigDataSE/ICESS* (pp. 1103-1108). IEEE.
[102] Singh, P.; Khan, B.; Vidyarthi, A.; Alhelou, H.H.; Siano, P. Energy-Aware Online Non-Clairvoyant Scheduling Using Speed Scaling with Arbitrary Power Function. Appl. Sci. 2019, 9, 1467.
[103] Khorsand, R.; Ramezanpour, M. An energy-efficient task-scheduling algorithm based on a multi-criteria decision-making method in cloud computing. Int. J. Commun. Syst. 2020, 33, e4379.
[104] Fernández-Cerero, D.; Jakóbik, A.K.; Grzonka, D.; Kołodziej, J.; Fernández-Montes, A. Security supportive energy-aware scheduling and energy policies for cloud environments. J. Parallel Distrib. Comput. 2018, 119, 191–202.
[105] Fernández-Cerero, D.; Fernández-Montes, A.; Jakóbik, A.; Kołodziej, J.; Toro, M. SCORE: Simulator for cloud optimization of resources and energy consumption. Simul. Model. Pract. Theory 2018, 82, 160–173.
[106] Vaquero, L.M.; Rodero-Merino, L.; Caceres, J.; Lindner, M. A Break in the Clouds: Towards a Cloud Definition; ACM: New York, NY, USA, 2008.
[107] Al Amri, S.M.; Guan, L. Infrastructure as a service: Exploring network access control challenges. In Proceedings of the 2016 SAI Computing Conference (SAI), London, UK, 13–15 July 2016.

Authors' Profiles

Md. Abul Hayat: He is a Cyber Security Ph.D. student at the Department of Computer Science & Engineering, IMT School for Advanced Studies Lucca, Piazza S.Francesco, 19, 55100 Lucca LU, Italy. Areas of interest: Cyber Security, Artificial intelligence, Cloud Computing, Software Engineering, Software Testing.
E-mail: abul.hayat@imtlucca.it

Sunriz Islam: She has completed her B.Sc. in Telecommunication & Electronics Engineering from Hajee Mohammad Danesh Science and Technology University, Basherhat, N508, 5200, Dinajpur, Bangladesh. One of her papers has been published recently. Now she is working on research in Networking, Cloud Computing, Cyber Security, and Artificial intelligence.
Email: sunrizislam@gmail.com

Md. Fokhray Hossain: Doctor of Sciences (Engineering), Full Professor, a Professor of the Department of computer science & engineering, Daffodil International University, Daffodil Smart City, Birulia 1216, Dhaka, Bangladesh. Areas of interest: Computer Fundamental, Computer Architecture and Organization, Enterprise Networks, E-Commerce and Web applications, Management Information Systems.
Email: drfokhray@daffodilvarsity.edu.bd

How to cite this paper: Md. Abul Hayat, Sunriz Islam, Md. Fokhray Hossain, "Securing the Cloud Infrastructure: Investigating Multi-tenancy Challenges, Modern Solutions and Future Research Opportunities", International Journal of Information Technology and Computer Science(IJITCS), Vol.16, No.4, pp.1-28, 2024. DOI:10.5815/ijitcs.2024.04.01