ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 12 N. 1 (2023), e31459
eISSN: 2255-2863
DOI: https://doi.org/10.14201/adcaij.31459

A Review of Cloud Security Issues and Challenges

Anamika Agarwal, Satya Bhushan Verma, Bineet Kumar Gupta

Department of Computer Science and Engineering, Shri Ramswaroop Memorial University, Barabanki, India, 225003
agrawal.anamika18@gmail.com, satyabverma1@gmail.com, bkguptacs@gmail.com

KEYWORDS

Security; Ransomware; Confidentiality; Data Encryption; Integrity; Availability; Authentication; Non-repudiation; Virtualization; Multi-tenancy; Denial of Service; Service Injection; Identity Theft

ABSTRACT

The advancement of information technology today depends on cloud computing. Every cloud consumer continues to search for the best services available, particularly in terms of security. The absence of uniform standards in the security architecture of the cloud, especially within the cloud computing community, has become an ongoing problem. Most cloud service providers automatically follow the best security practises and actively protect the operation of their systems. Enterprises are required to independently judge the security of their data, apps, and the cloud's workload. The complexity of security concerns is increasing as the digital environment develops. Virtualization, multi-tenancy, security controls, rules, and risk profiling are all concepts in cloud security. DoS, service injection, user-to-root attacks, man-in-the-middle attacks, data loss leakage andloss, identity theft, and backdoor channel attacks are a few of the dangers associated with cloud computing. Cloud platforms, data outsourcing, data storage standardisation and security, data backup, and data recovery are all examples of cloud security services. Data storage, computation, untrusted computing, and virtualization security challenges are all a part of the cloud.

1. Introduction

India is becoming digital and more connected over the Internet. The amount of internet users is increasing every day and is currently at over 800 million. This year, due to the launch of 5G, this number is expected to increase drastically. With an increasing number of users there isa greaterchance of cyberattacks, in other words, users'devices are becoming more vulnerable. Online users need to be more cautious in this digital era especially those who are not familiar with technology. As Norton Labs (2022) had predicted, the need for online security professionals had increased in 2022 due to new types

of cyberattacks. Regarding recent cyberattacks, the statistics are no less shocking. About 40.9 billion email threats, malicious files and URL were blocked during the first half of 2021.This data was given in the report of a global cybersecurity firm Trend Micro.Globally, ransomware is the biggest threat. In 2022, ransomware accounted for12% of total cybercrime attack of ransomware cases in India.

The technology of cloud computing has attracted a lot of interest worldwide. It provides services through the internet, enabling users to access the online services of other software without having to buy or install it on their own computers. The increased demand for organisations to supply services was one of the driving factors which have led to the emergence of cloud computing. However, because data and resources in the cloud are kept and managed in the datacentres of third-party cloud services providers (CSP), data privacy and security are top issues for cloud customers. Furthermore, cloud users connect to the cloud through the Internet; if they did not have an internet connection, they would have been unable to access their documents and apps on the cloud, which would result in monetary loss for the user. The same problem arises in the case of cyberattacks on different clouds. Although new cybersecurity technology is emerging every day so do new attacks. Thus, we have to work on a resilience security framework which means that whenever an attack happens, we should be able to detect itvery fast, and segment a part of the system; this can be compared to amputating a damaged part of the body, the procedure is carried out so that the rest of the body can survive. Once the issue is resolved, the segmented part is reattached to the system so that itcan go back to working as normal.

The need for a cloud security framework is justified asfollows:

- Standards, methods, practises, and procedures for cyber risk management must be integrated in a framework that links business, policy, and technological perspectives.
- A targeted, repeatable, flexible, cost-effective, and performance-based strategy, including information security controls and measures, must be provided to assist critical infrastructure operators and owners in assessing, identifying, and managing cyber risk.
- Areas that require further development must be identified so that they may be addressed in future partnerships with particular sectors and organisations, and standards may be set.
- International voluntary standards should be complied with.
- There should be a shift in focus from compliance to action and a specified objective.

This framework is a voluntary set of standards that are designed to help firms better manage and lower their cybersecurity risk. It has been built on current best practises and guidelines (Subramanian et al., 2018; Mell et al., 2018; Xu X 2012; Pippal et al., 2013). Cloud computing has received a lot of attention recently as a result of the rising demand in the last decades. Businesses that switch to cloud-based data storage solutions may benefit in a number of ways. These benefits encompass simplified infrastructure administration, the ability to access resources remotely from nearly any location with a dependable internet connection, and the potential for cost reductions via cloud computing. Further investigation is necessary to tackle the security and privacy challenges associated with cloud technology. Previous research efforts, involving scholars from academia, business, and standards organizations, have suggested potential solutions to these challenges. The aim of the current study has been to explore the various facets of cloud computing while also addressing the privacy and security requirements and apprehensions linked to cloud services, along with their recognized threats and vulnerabilities. This study also identifies potential security solutions andproposes a new categorization of those solutions. This paper helps to identify the security issues faced by cloud companies, cloud suppliers, cloud data owners, and cloud clients. Services are classified into three unique models, as shown in figure 1:

- **Platform as a service (PaaS)**: This cloud services concept refers to a third-party supplier granting customers online access to computer hardware and software resources. These resources are often required for the development of apps. The hardware and software are housed on the PaaS provider's infrastructure. By using PaaS, developers may avoid the difficulties associated with setting up on-premises hardware and software to build or execute new apps and provide access to users or cloud-based programmes and systems (Soofi et al., 2014).
- **Software as a service (SaaS):** In certain contexts, also referred to as on-demand software. It is a runtime environment paradigm where a cloud provider offers solutions. Users and developers do not need to download and install these services on their devices in order to use them because they are available to end users over the internet. It provides readily available services (Soofi et al., 2014).
- **Infrastructure as a service (IaaS)**: That is one of the platform levels for cloud services. IT systems, including servers, networking, computing, storing, virtualization software, and other resources are available for customers to outsource. Customers pay for these resources on a per-use basis in order to access them online. IaaS provides processing, storage, and other computer resources as a service (Soofi et al., 2014).

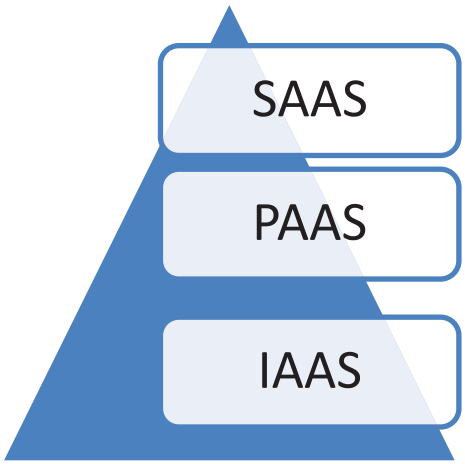

Figure 1. Service delivery models for cloud services

Security Administration

All activities required to safeguard, recuperate, and ensure the security of information in computer networks are encompassed in the concept of internet safety. By and by, security instruments carry out security strategies through the security administrations they offer. Administrations such as respectability, classification, confirmation, non-renouncement, and accessibility help to expand the security of computerorganizations and data systems (Romani et al., 2018). The evaluation of the computing architecture is shown in figure 2.

- **Secrecy:** Ensures that no data is revealed or made available to strategies, gatherings, or individuals that are not approve. Information transmission (and gathering) ought to limit access by unapproved parties.

- **Information encryption:** A valuable procedure for protecting security. For encryption, either an unbalanced key worldview or a symmetric key worldview can be applied.
- **Integrity:** Ensures that the data received by a reliable party is an indistinguishable reproduction of the data that was first given. It guarantees that no other person has modifiedthe information, be it purposefully or unintentionally. Attackslead to invalid information being sent.
- **Availability:** Ensures that administrations are accessible to approved clients and that, upon demand, approved organisations may gain access and use the information. For example, in the event that a framework is the objective of a conveyed distributed denial-of-service (DDoS) attack, giving data will not be able.
- **Authentication:** Authenticates the user of the information, the sender and the receiver. Information integrity and secrecy are only significant whenever the identity of senders and recipients is correctly confirmed.
- **Non-repudiation:** Ensures that neither the shippers nor the beneficiaries may question the moves made. Source and objective renouncement are the two classes into which disavowals are separated. In the former, neither the source nor the beneficiary can challenge the data transmission, while in the latter, neither can challenge the transmission of the message.

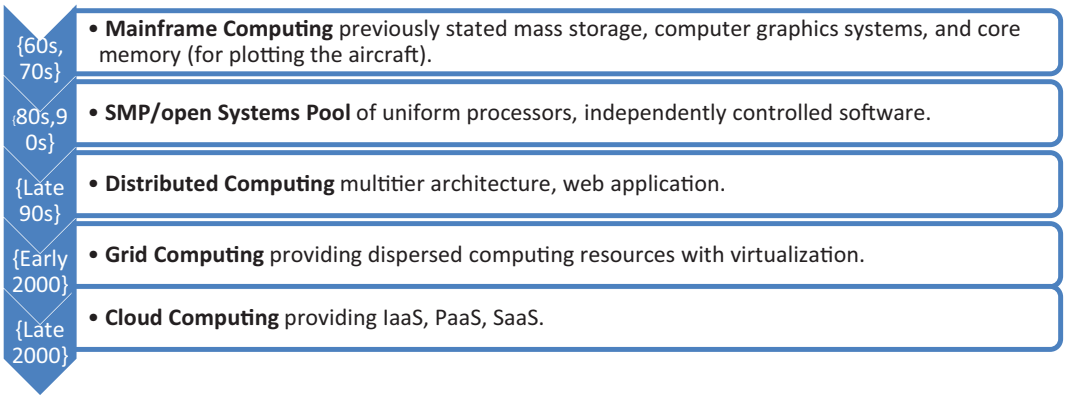

Figure 2. Evolution of the computing architecture

Cloud computing employs three primary delivery methods: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS). SaaS primarily focuses on providing access to applications. PaaS offers a development platform as a service, which can support the creation of higher-level services. IaaS offers fundamental processing and storage capabilities as standardized network services. This cloud deployment model offers a distinct type of cloud environment characterized by its flexibility, ownership options, and accessibility. There are three primary deployment model types: public, private, and hybrid clouds. Private clouds are hosted within an organization's own data centres, while public clouds are provided by external entities such as government agencies, industry providers, or academic institutions. Hybrid clouds combine a private cloud with one or more public cloud services. Each approach has its unique advantages and disadvantages, with private clouds offering organizations complete control over user management. Security responsibilities for the cloud infrastructure and the applications it hosts are shared between the cloud provider and the cloud user. The

user is also responsible for creating, provisioning, and deactivating user accounts, as well as managing password policies, server-level authentication processes, and other related tasks. Interestingly, only 43% of respondents correctly identified the most popular IaaS shared responsibility security approach, as reported in the Oracle and KPMG Cloud Threat Report (2018). Organizations are advised to employ a range of network security measures, including physical and virtualized firewalls, intrusion detection and prevention systems, gateways, and deliberate workload and cloud application restrictions. Furthermore, 66% of respondents reported experiencing a cybersecurity issue.

Cloud configuration

The cloud settings are covered in the following paragraphs with the aim of providing a better understanding of security risks. A cloud business is composed of resources that are devoted to requests. According to nits, the following five primary actors make up a cloud computing configuration:

- **Cloud consumer:** Clients can choose lower expenses and better administrations by consenting to a service-level agreement (SLA) with a cloud supplier.
- **Cloud provider:** A cloud provider is an individual or organisation thatenables a cloud client to access support. The cloud supplier puts together and organizes cloud programming by buying and dealing with the cloud framework. To offer administrations the expected assistance levels while using SaaS, the cloud supplier conveys, designs, keeps up with, and redesigns the product applications. The platform's computer infrastructure is managed by the cloud provider under PaaS (platform-as-a-service).
- **Cloud auditor:** Freely assessing cloud administrations is the obligation of a cloud examiner. To decide whether norms have been met, the inspector checks the cloud objectively. The presentation, security, privacy, andcloud administration may be generally evaluated by cloud auditors.
- **Cloud broker:** Cloud brokers are responsible for managing interactions between cloud users and cloud providers as well as the use, performance, and delivery of cloud services. Service aggregation, service arbitrage, and service intermediation are the three service categories they offer. Service intermediation improves a particular service, as opposed to service aggregation, which merges or integrates several services into one or more new services. The broker is free to select services from several suppliers while using service arbitrage.
- **Cloud carrier:** A cloud carrier acts as an intermediary connecting cloud providers and customers to deliver cloud services. Cloud carriers establish connections with customers through networks and other access points. As mentioned earlier, when cloud providers establish Service Level Agreements (SLAs) with a cloud carrier, the cloud provider may deliver services that are in compliance with SLAs to cloud clients. In addition, the cloud carrier is responsible for allocating reliable connections to both cloud users and providers.

Figure 3 provides an outline of the NIST cloud computing framework (Patil et al., 2019), including a roster of key participants, their functions, and their respective roles within cloud computing. This visual representation effectively highlights the prerequisites, attributes, and benchmarks pertinent to cloud computing. It also serves as a basis for evaluating the performance attributes of services. Nonetheless, it's crucial to note that Service Level Agreements (SLAs) do not ensure the delivery of a specific service (NIST, 2011). In other words, SLAs cannot mitigate the risks associated with selecting

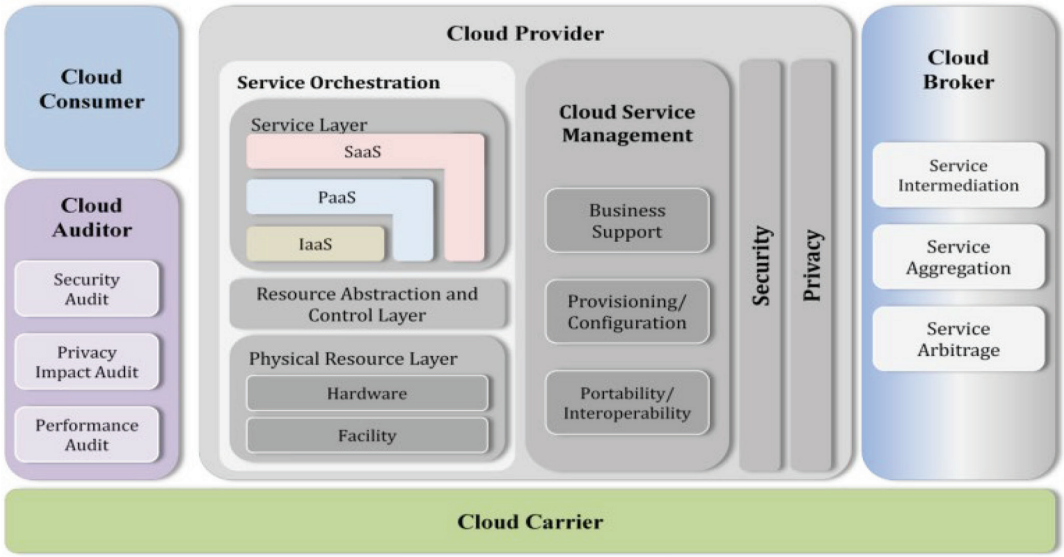

Figure 3. NIST setup for cloud computing (Patil et al., 2019)

a subpar service or transform an inferior service into a superior one. SLAs frequently detail potential complaints and list the services they cover. The client's and service provider's duties are simultaneously set under the SLA. The availability, data usage, service provider's response time, and specific performance criteria are all specified in the SLA (Fotiou et al., 2015).

2. Related Work

In terms of data security, access control, and other challenges, cloud computing represents a new paradigm for computers (Yu et al.,2010). Over the past few years, extensive research has been conducted regarding security concerns within the realm of cloud computing. Furthermore, it is evident that the majority of the examined papers have made substantial contributions to addressing challenges in cloud security. These notable works have proven highly valuable and comprehensive in advancing research within this domain.

Kavin et al. (2020) offered safe cloud storage and recovery, it is possible to efficiently guarantee secure data transfer. As far as security level and execution, the preliminary discoveries additionally showed the adequacy of the proposed reinforced security design.

Tabrizchi et al. (2020) conducted an investigation of state-of-the-artsecurity systems. To lessen risk and susceptibility and boost confidence in a constantly linked world, the article gave a number of written rules, procedures, and processes that define the safe management approach in the cloud environment.

To shield high-risk VMs from malware at an early place of the VMlife cycle, Patil et al. (2019) introduced an in-VM-helped lightweight specialist-based malware identification framework. It used both mark-based identification at the VM layer and oddity location at the hypervisor layer, permitting

it to distinguish both known and unidentified malware. Another advantage is that it onlygave profiles of malware that were obscure to the hypervisor layer, for oddity recognition, subsequently limiting transmission costs.

Sgandurra et al. (2016) made a scientific classification of attacksin virtualized frameworks in light of the source, the attackers' points, and the casualty at different levels. The authors demonstrated how dangers have developed alongside related security and trust issues in virtual servers across various layers, including equipment, working framework, and application.

A framework of safety issues with cloud computing was introduced by Kaur and Singh (2015). Concerns regarding the information area, capacity, security, availability, and respectability were canvassed in this article. The study focused on fundamental security issues; however, it is critical to underline that the creators simply examined security vulnerabilities without recommending practical solutions.

In addition to demonstrating a way for resolving security issues in a multi-tenant environment, Kumar et al. (2018) also highlighted a variety of data security obstacles in cloud computing. Actually, the entire focus of this essay was on issues with data security and methods for maintaining privacy and data security.

A meta-analysis of security and privacy concerns with cloud services was provided by Khalil et al. (2014). This study classified numerous kinds of cloud vulnerabilities as well as various recognised security hazards and attacks. This review study also covered potential future security threats and examined the flaws in existing remedies.

A thorough analysis was conducted by Bashir et al. (2011) to pinpoint the security issues with cloud computing that are most likely to arise. This research study also analyses significant security concerns related to cloud computing for end users and vendors by providing analysis linked to various security models and technologies.

In their survey, Ryan (2013) outlined important research goals, including a data protection policy that aims to secure data from cloud platform providers. Furthermore, a software-as-a-service application can supply secrecy services using the technique described in this research for browser key translation. One of the long-awaited realisations of computers as a utility is cloud computing, which offers high-quality services from a shared pool of adaptable computing resources (Wang et al.,2010). With cloud computing, customers may remotely store their data. Because the vast majority of cloud-related technologies have made significant strides in the modern world, security concerns have changed, and new problems have arisen. It is therefore necessary to do in-depth research, identify potential problems, and create novel solutions.

Ransomware attack vectors utilized for monetary benefit and danger entertainers chasing after new attack surfaces were examined by Naik1 et al. (2019). The study finished by scattering an interminable measure of polymorphic ransomware tests while the guilty parties escaped identification. Furthermore, it was inspected whether the writers of ransomware danger entertainers shared a typical composing style or different qualities that could be utilized to assist with distinguishing them. Gathering a few ransomware tests in view of practically zero data about them permits specialists to explore and distinguish their highlights and marks, which is the most important phase in attempting to recognize the attack's source. To sort out ransomware tests, this examination prompted utilizing two fluffy strategies: fluffy hashing and fluffy c-implies (FCM) bunching. Unlike other bunching procedures, FCM does not need extra groundbreaking moves toward assemble object distance to organize things into practically identical gatherings. The similarity scores generated by a fuzzy hashing method may be used directly instead. It lessens the computational overheads by utilizing fluffy comparability scores assembled

during the main emergency of whether the example is known or obscure ransomware. The presentation of the proposed fluffy procedure was differentiated against k-implies grouping and the two fluffy hashing strategies, namely, SSDEEP and SDHASH, were surveyed in light of their FCM bunching results, to comprehend how the closeness score impacted the bunching results.

Wilson et al. (2021) stated thatransomware was the kind of cybercrime that grew the fastest and was a huge security risk for organizations. Information on a hacked computer is encoded by traditional ransomware, keeping clients from getting to it until a payment is paid. Double-extortion ransomware operations, in which files are first seized and then encrypted, can still generate income by extorting the firm or, if a higher ransom is not paid, by selling any sensitive material on the dark web. Enterprises cannot be shielded from these new types of data theft and extortion firm by firewalls, antivirus software, and regular backups. To find and destroy this danger, intelligence analysts and proactive cyber threat hunters are required.

Singh et al. (2020) proposed a software-defined perimeter (SDP) as a method for shielding IaaS, giving a sensible limit validation and approval to confine admittance to administrations. Results demonstrate that SDP can endure DoS attacks regardless license genuine client traffic even when the attack is continuous.

Lee et al. (2016) pointed to ransomware attacksbecoming progressively common, with messages being the essential meansfor their spread. The authors provided an improved ransomware insurance framework based on an investigation into CloudRPS's abnormal conduct. The authors also proposed an identification framework, which was able to perform continuous organization, record, and server checking. Likewise, a cloud framework was set up to accumulate and inspect information from the device and log information to forestall attacks.

Suthar et al. (2017) stated that cloud computing gives clients admittance to various administrations ata minimal expense; however, clients should beguaranteed that their information is secure. Cloud specialists are working autonomously to resolve this issue, however, most exploration propositions centre around client-side security-related issues. This paper exploredthe model with two techniques that's Data Obfuscation for server side to secure database details from outsiders and Encryption, authentication at client side to guarantee that clients and specialist co-ops can depend on each other.

The review of Singh et al. (2017) highlighted that cloud computing delivers on-demand services via the Internet, offering cost-effective solutions and scalability. Nonetheless, the transition from local to remote computing has introduced security apprehensions and challenges for both consumers and providers. This study discusses the fundamental characteristics of cloud computing, security concerns, dangers, and remedies. It also covers a wide range of open research questions concerning cloud security.

Sun et al. (2020), discussed Cloud computing security and privacy protection, with research progress on privacy security challenges and a strategy for protecting against risks.

Kumar et al. (2019), presented a comprehensive approach involving the holistic alignment of cloud security needs, identified threats, established vulnerabilities, and suggested remedies. They also introduced a standardized classification system for security requirements, threats, vulnerabilities, and solutions.

3. Cloud Security

Computer security encompassescloud security (Singh et al., 2016; Khalil et al., 2014; Ahmed et al., 2018). It determines an arrangement of guidelines, controls, and innovations that are helpful for defending information and administrations. The cloud framework is influenced directly or indirectly by

dangers and attacks. The compromise of the cloud resources' integrity, availability, and confidentiality, as well as the services provided by various levels, may generate new security concerns. Our objective in this section is to look at various security concepts that help to obtain a more in-depth comprehension of cloud security concerns. Summary of the cloud security mention in the figure 4.

3.1. Standards of Cloud Security

Cloud security tends to an assortment of safety issues and dangers. The review investigates the reason for the weaknesses and vulnerability to understand cloud security. This section talks about specific cloud-explicit issues, such as virtualization, multi-tenure, cloud stages, information rethinking, information capacity normalization, and trust management, to better understand the security issues that are common in the cloud.

3.1.1. Virtualization Component

Virtualization is the process of isolating administrations, applications, registering assets, and working frameworks from the real equipment on which they are put. A virtual machine (VM) is a picture that contains a significant part of memory and capacityof the guest operating system. Virtual machine management (VMM) gives each VM virtual equipment assets, and the VMs are associated with the interior and outer organizations by means of virtual switches. VMware and vSphere are two stages that offer virtual usefulness. VM pictures are fast and simple to move, duplicate, and create clones, and clients can help exceptionally available and versatile administrations through the cloud.

3.1.2. Multitenancy

The notion of sharing is introduced by a feature of the cloud computing environment called multi-tenancy, which enables one or more tenants to share each operating instance. It makes it feasible for some individuals to share a solitary cloud stage. While examining an IaaS supplier, VMMs alludes to a stage for multi-tenancysharing, while VMs alludes to the examples. Clients can run various projects, including the.NET System and Java virtual machine (JVM), on the virtual platform (VP) of a PaaS supplier in a multi-tenancysetting. Co-occupancy, co-area, and co-home attacks can be utilized to exploit multi-tenure since buyer important information might be available at a similar actual spot. They permit an attacker to get to neighbouring virtual computers or running projects.

3.1.3. Threat Agents

Threat agents are elements which can fight off an attack and create threats. Whether it happens inside or remotely, this danger is brought about by an individual or any product program. Ananonymous attacker, for example, an outer programming system or outside human, utilizes a public organization to send an organization level attack. Untrusted cloud administration clients are the people who use the cloud climate without the director's authorization.

Malevolent service agents are bits of programming that block messages, have an outside presence, and have rationale that is either hacked or noxious. It may be possible to move or transfer network traffic flow in a cloud. A believed attacker is a confided cloud client who utilizes the common IT assets of a similar cloud foundation. The dependable attacker enters the cloud trust hindrance by utilizing a client's legitimate qualifications to send off their attack. Malicious insiders are the people who represent a danger to cloud specialist organizations. They regularly act as delegates of an outsider or

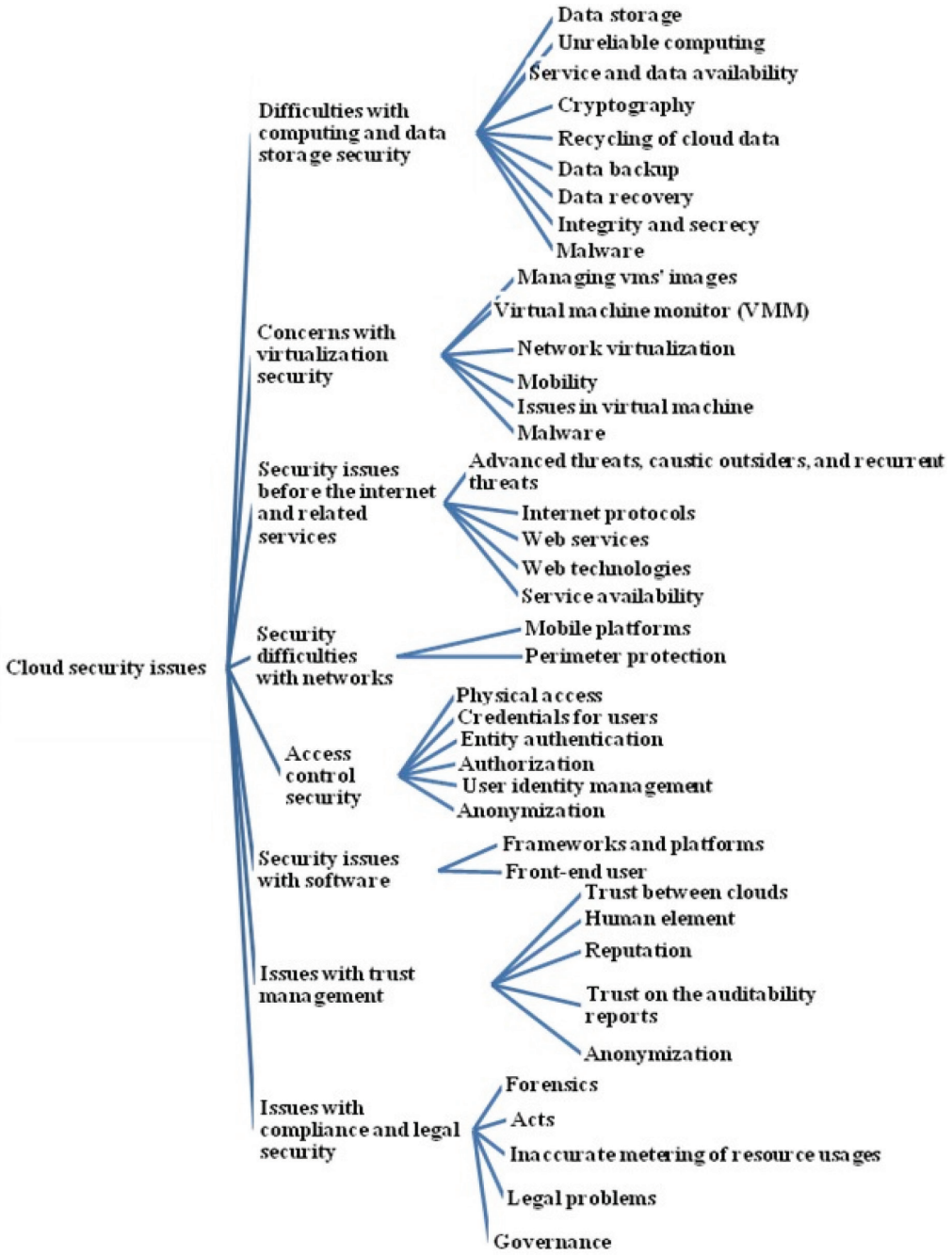

Figure 4. Summary of Cloud Security

representatives of the cloud supplier firm. This kind of attack is very unsafe since it could be feasible to get authoritative admittance to IT assets used by cloud clients.

3.1.4. Security Controls

Security safety measures must be implemented ahead of time to diminish or eliminate risk. The countermeasures likewise forestall or moderate security dangers. A list of security countermeasures, how to apply them, and other relevant information are all included in the security policy. It contains various prescribed procedures and standards for carrying out security controls for a framework, administration, or security plans. The security rules permit us to get delicate data and significant assets completely.

3.1.5. Security Mechanisms

IT resources, sensitive data, services, and information are all protected by security measures, which are a type of defensive framework. To increase the security of the system, security mechanisms are characterised in terms of safeguards and countermeasures.

3.1.6. Security Policies

An assortment of safety rules and guidelines are laid out using security strategies. This security strategy expounds on how these rules are placed into impact in a security framework. Security arrangements, for example, may help clarify the position and use of safety controls and methodology.

3.1.7. Cloud Security Administrations

The cloud security administration is a blend of a service, strategy, regulation, and behaviour intended to safeguard IT assets. It encompasses five fundamental security services: confidentiality, data privacy, user authentication, integrity, and validation. Authentication can be compromised through weak passwords, simple recovery methods, and unsafe registration procedures. Cloud computing's high availability feature aims to minimize application downtime and avoid business disruptions. It is the responsibility of the cloud provider and cloud carrier to ensure that cloud IT resources are accessible in a cloud computing environment.

3.1.8. Cloud Platforms

When cloud users intend to deploy their applications and services on cloud platforms, they require practical strategies and tools to assist them. For instance, in the case of Infrastructure as a Service (IaaS) offerings, the cloud platform relies on Virtual Machine Managers (VMM), which provide a virtualized layer. As a development environment for Platform as a Service (PaaS), platforms like.NET and JVM are commonly utilized. These platforms supply the necessary tools for creating Software as a Service (SaaS) applications. To facilitate the development of cloud applications, the platform offers Integrated Development Environments (IDEs) and Application Programming Interfaces (APIs). These tools are built upon the foundational elements of the platform and its programming languages.

3.1.9. Outsourcing of Data

For business purposes, organizations currently employ outsourced data models, which refer to a method wherein users delegate data collection and extraction responsibilities related to a specific

subject to a third-party provider. This third party often engages with various companies, offering both capital and operational investment. Many IT industries have embraced the concept of data outsourcing, which serves the IT sector with data management, processing, storage, and security services. One challenge with this data outsourcing approach is that it effectively severs the connection between the data owner and their data. When a consumer entrusts their data to a third party initially, they do so to ensure that data processing and storage occur securely, as the user relinquishes some control over the data.

3.1.10. Standardization and Protection of Data Storage

The OSI worldview integrates security methods, such as computerized marks, validation frameworks, and conventions. It also requires secure information storage and strategy support. Mists disseminate information among different data centres, allowing a copy of the information to be distributed across various data centres. The 3-2-1 rule is a commonly used information reinforcement idea.

3.1.11. Trust Management

The component of confidence in cloud security isn't quantifiable. It allots the equipment, network design, foundation, and data centres to itself in light of the decisions. Various elements, including complex and multi-staged events, are utilized to assess trust. Along these lines, trust is extremely sporadic and in light of the basic element. The trust issue in cloud computing arises because of the far-off area and outsider treatment of shopper information and administrations.

3.1.12. Identification of Security Threats

The hardest piece of executing a practical countermeasure in an is sorting out the particular security dangers. Distinguishing security chances and the comparing security needs are the underlying strides in the standard security framework creating process. Chosen security controls are then applied to track down elevated degrees of unwavering quality, practicality, and legitimacy. The establishment for building any security framework is the secrecy, honesty, and accessibility. To make a protected cloud, certain essential security parts should be utilized. The high accessibility, centralization of safety, overt repetitiveness, and division of information and cycles are a couple of the security benefits presented by the cloud engineering plan.

3.2. Security Necessities for the Cloud

The necessities for cloud security are talked about in this subsection (Sumitra et al., 2014; Fernandes et al.,2014; Subashini et al.,2011). Prior to utilizing any of the administrations, every business association settles on a security technique choice. Accessibility, privacy, respectability, non-disavowal, and verification or personality are the other five security rules. Each assistance model (IaaS, PaaS, and SaaS) requires approval for public clouds to forestall unauthorised access. It is more protected than both public and private clouds in light of the fact that the mixture cloud engineering requires stricter security prerequisites. Furthermore, the reconciliation prospects increment security in the hybrid cloud. Respectability is a significant prerequisite for all cloud security models to confirm that the information is exact. Application insurance is given by the SaaS security worldview for applications with administration and electronic access. Because of the great accessibility and uprightness of the administrations, strong safety efforts in the basic organization were fundamental.

3.3. Cloud Computing Threats

From a computer security standpoint, anything possessing the potential to cause substantial harm to a computer system is deemed a threat. These threats can potentially culminate in attacks against the computer system or network infrastructure. Hubbard and Sutton's paper from 2010 delineated the most prominent threats to the security framework of cloud services. As depicted in table 1, the article enumerates various potential hazards associated with the cloud.

Table 1. A thorough investigation into the problems raised by the CSA's 2013 report on cloud security threats

Threats	**Effects**	**Affected Cloud-Services**	**Solutions**
Various service delivery and receipt models	Cloud infrastructure losing its ability to be controlled.	SaaS, PaaS and IaaS	Offered regulated and restricted services.
Cloud computing abuse and malicious use	There is a loss of validation, service fraud, and a greater attack as a result of confusing sign-ups.	IaaS and PaaS	Use robust registration and authentication techniques while keeping an eye on the network's health.
API and interface security issues	Incorrect transfer of the content, improper authentication, and authorization.	SaaS, PaaS and IaaS	Strong access control and authentication measures are used, and data transfer is secured.
Malicious insiders	Resource penetration, asset damage, productivity loss, and operational impact.	SaaS, PaaS and IaaS	Utilization reporting and breach alerts, as well as open security and management procedures.
Shared technology issues	By exploiting the hypervisor, interfere with one user service and other user services.	IaaS	For administrative duties, use robust authentication and access control processes and audit settings and vulnerabilities.
Data leakage and loss	Personal information about you might be changed, removed, corrupted, or wiped.	SaaS, PaaS and IaaS	Methods for storing and backing up data.
Service or account theft	The security of a services is at risk when user account information is stolen since it grants access to a key area of the cloud.	SaaS, PaaS and IaaS	Use of strong authentication methods, security best practises, and encrypted communication.
Risk assessment	Internal security procedures, security standards, configuration breaches, patch, audit, and log.	SaaS, PaaS and IaaS	Recognize incomplete logs, infrastructure, and data components to protect the system for tracking and changing how data is used.
Theft of identity	To access that user's resources and obtain credits or other benefits under that username, an attacker can obtain the identity of a legitimate user.	SaaS, PaaS and IaaS	Use strong multi-tier passwords and authentication procedures.

3.3.1. Different Service Receipt and Delivery Models

Both the business model and the cloud computing paradigm employ distinct approaches to delivering and receiving services. Consequently, cloud computing possesses the adaptability to modify its own service delivery approach. As the provider of cloud services has outsourced all services and applications to a remote location, businesses must carefully evaluate the risks associated with relinquishing control over the cloud. Cloud data traverses between two distinct locations, each governed by its own set of security protocols. This presents a primary concern that arises when utilizing such services. Mitigating these risks necessitates the implementation of robust end-to-end encryption, universally accepted security standards, and a trust management system.

3.3.2. Cloud Computing Malicious Use and Abuse

IaaS providers offer these utilities, which include unlimited network, storage, and bandwidth resources. Some service providers allow users to try out their offerings for a predetermined trial period. This often involves a straightforward registration process that grants access to cloud services without requiring an extensive security verification. During the trial period, users typically have limited control and influence over security measures. Potential threats encompass Distributed Denial of Service (DDoS) attacks, password and key cracking attempts, captcha-solving farms, and hosting of hazardous materials. These vulnerabilities may be exploited by spammers, creators of malicious software, and other malicious actors for launching their attacks. These risks pose a potential threat to the infrastructure of both IaaS and PaaS services. Therefore, during the initial registration process, it is imperative to implement robust authentication mechanisms, appropriate validation procedures, and thorough verification measures to safeguard the cloud against such risks.

3.3.3. API and Interface Security Issues

Cloud users have the option to interact with cloud services through a set of software interfaces and APIs provided by the cloud provider. These interfaces add a layer of complexity to the cloud architecture as they are deployed atop the core cloud infrastructure. They empower users with comprehensive provisioning, management, and monitoring capabilities. Therefore, the security of these APIs plays a pivotal role in ensuring the availability and safety of the cloud environment. However, the security of these APIs can be compromised at times due to both intentional and unintentional actions. Such API attacks can have repercussions on PaaS, IaaS, and SaaS service models. Furthermore, since other entities often build upon these interfaces to offer services to their clients, an additional layer of risk may be introduced. This risk can be mitigated through the implementation of robust access control mechanisms, authentication protocols, and secure interface designs.

3.3.4. Malicious Insiders

Malicious insider threats pose significant risks in cloud computing, primarily due to the fact that many companies do not divulge information regarding their hiring practices and the extent of their employees' access to internal resources (Zhang et al., 2017; Abbas et al., 2017). This threat is primarily fuelled by a lack of transparency and the convergence of IT services and user management within a single domain. Consequently, employees often enjoy heightened access to data, leading to breaches

of confidentiality for both services and data. Moreover, this situation creates opportunities for insider attackers to gain access to critical data and disrupt cloud services.

This scenario can be initiated by an insider attacker who can gain unauthorized access to the system through the firewall or intrusion detection system, exploiting a situation where the security system perceives their activity as legitimate.

3.3.5. Issues with Shared Innovation in a Multitenancy Setting

IaaS suppliers utilize the idea of virtualization to offer support in a multi-tenancy setting. Through virtualization, it is achievable for a few people to have a similar asset. The hypervisor in a multi-tenancy framework could unveil client data to an unapproved client. Since the framework was not intended to offer dependable separation in a multi-tenancy environment, there is a huge risk included. The idea of sharing could influence the cloud framework overall by permitting one client to see information about another client. Access control major areas of strength for and are two tools for forestalling this issue.

3.3.6. Data Leakage and Loss

Data loss happens when information is erased, changed, or taken without a backup of the original content. Since cloud computing is so cooperative and compelling, missing an encoding key may possibly prompt data loss. The significant explanations behind data loss and leakage incorporate a shortfall of authentication, authorization and access control, deficient encryption techniques, delicate keys, the probability of affiliation, a temperamental data centres, and an absence of calamity recuperation. These weaknesses could meaningfully affect the IaaS, PaaS, and SaaS administration models. Utilizing secure APIs, protecting information honesty, utilizing secure capacity, utilizing strong encryption keys and calculations, and sponsorship up your information are a couple of precaution measures (Kalaichelvi et al., 2015).

3.3.7. Service /Account Theft

The purchaser might be effectively controlled to a dangerous site during the help capturing process. Fraud, phishing, and the use of programming bugs are techniques that might be utilized to achieve this. Reusing login accreditations and passwords normally brings about these attacks. In cloud computing, on the off chance that a programmer accesses a client's certifications, they can record ways of behaving, alter information, return misleading data, or guide clients toward compromised accounts and deceitful sites.

3.3.8. Assessment of Risk

Cloud services are less taken part in the proprietorship and upkeep of equipment and programming because of the great responsibility. The cloud gives organizations an agreement for keeping up with their product and equipment. Albeit this idea is sound, cloud computing can't fathom an organisation's inner security rehearses, like fixing, evaluating, security approaches and logging processes (Fan et al., 2013). There are extra perils and risks because of this obliviousness. The cloud ought to incorporate a screen and changing framework as well as comprehension of some architecture details, logs, and information for the disposal of dangers.

3.3.9. Identity Theft

Identity fraud is a sort of misleading in which somebody expects the identity, resources, credits and different privileges of another person. Threats like this have a lot of bad consequences for the victim, who also loses. This peril might come from keyloggers, phishing plans, insufficient secret word recovery strategies, and different issues. The security approach incorporates multi- tiered authentication techniques and secure secret key recovery systems.

3.4. Attacks on the Security of the Cloud

The advantages of Cloud computing are known by organizations. There are continuously arising innovations that present new dangers to Cloud computing. New dangers have without a doubt showed up since cloud framework took on new innovation. At the point when a cloud takes on new cloud innovation, a few attacks are sent off. The table 2 records numerous security breaks, their consequences for the cloud, and several potentialsolutions.

Table 2. Thorough investigation of cloud attacks with solutions

Threats	**Attack Surface and Procedure**	**Affected Cloud Services**	**Effects**	**Solutions**
Denial of service attack	Attacks against the VM and hypervisor, the host being inundated with direct or indirect SYN packets, and network-based attacks.	PaaS, IaaS and SaaS,	If service availability is compromised, a fake service could be formed.	Dependable authorization and authentication.
Attack using service injection	Distracting service entry via application and VM level attacks, obtaining service identification files.	PaaS	Service integrity is compromised, and users are given malicious services in place of legitimate services.	API security, strong isolation techniques across VMs, hash function to verify service integrity, use of secure online browsers, and web service security.
A virtualization attack	Separation of the virtual layers in agreement with the hypervisor. Attack on the hypervisor and VM levels.	IaaS	Acquire the login details and delegate authority to another user.	Need for hypervisor security solutions, monitoring of hypervisor activity, and requirement for VM isolation.
A user-to-root attack	Accessing every resource that a legitimate user has. User-level violence.	SaaS	Obstruct the privacy of sensitive client information and services.	Create secure passwords and use stronger authentication methods.

Table 2. Thorough investigation of cloud attacks with solutions (continued)

Threats	Attack Surface and Procedure	Affected Cloud Services	Effects	Solutions
Port scanning	Examine the open port to learn more about it.	PaaS, SaaS, and IaaS	Unusual service behaviour reduces service availability.	Strong port security is necessary.
Attack by a man-in-the-middle	Gaining access to two-person data transmission.	PaaS, IaaS and SaaS	Breach data security and privacy.	It was important to use an adequate, secure Secure Socket Layer (SSL) architecture.
Attack on spoofing metadata	Service level attack: alter service information files, such as WSDL.	PaaS, SaaS	Abnormal service behaviour compromises service privacy.	A strong authentication method was required to access the file, and service functionality and other data should be preserved in encrypted form.
Attack by Phishing	Using a false website link.	PaaS, SaaS, and IaaS	A user's sensitive personal data that shouldn't be shared.	Employ a secure web link (HTTPS).
Attack through the backdoor	Settlement of the VM and hypervisor level attacks, as well as the valid user VMs.	IaaS	Give rights for obtaining legitimate user resources, impact service availability and data privacy.	Strong authentication, identification, and isolation procedures are necessary.

3.4.1. Denial of Service Attack

An attack known as a denial of service (DoS) is when an attacker bombards with many request packets through the Web to exhaust the casualty of every accessible asset. These packet types include user datagram protocol (UDP), transmission control protocol (TCP), and internet control message protocol (ICMP) echo request packets. The SYN flood attack is the most pervasive, while the Smurf attack involves sending ICMP "Echo request" packets to a victim port that isn't open for tuning in. The DDoS attack is more perplexing and testing to distinguish than a DoS strike, as the culprit of a DDoS attack would first search the entire organization for powerless servers and reach out to them.

3.4.2. Attack Using Service Injection

A cloud framework offers the types of assistance to its client. To utilize a help, a client should initially present a solicitation to the cloud framework, which is then liable for making the necessary assets openly accessible. A later requester might get the additional asset that was first designated to the individual who started the solicitation. Another malevolent picture of the designated asset is created each time an attacker attempts to present a malicious asset, administration, or new virtual machine into the cloud climate. The malicious service acts like a cloud administration when a client demands an

assistance. The genuine usefulness of the cloud might be impacted by this. To safeguard against this type of attack, a service integrity module implementation is required.

3.4.3. A Virtualization Attack

In the cloud, virtualization dangers take two primary structures. A hypervisor rootkit is the second, and VM escape is the first. During a virtualization attack, control of the virtual machine in the virtual climate will be taken. A zero-day attack is one of the techniques. Different dangers incorporate multi-tenure, VM control, capacity portion, and indirect access channel attacks.

3.4.4. A User-to-Root Attack

The attacker or gatecrasher in this attack gets full admittance to the entire framework by getting the record and secret key of an approved client. This kind of attack utilizes information that has spilled or been added to a statically characterized support.

3.4.5. Port Scanning

Utilize port examining to figure out which framework parts are open, shut, and sifted. Programmers utilize open ports from connections, including services, IP addresses, and MAC addresses, during port examining to take data. The most widely recognized types of port filtering attacks incorporate TCP, UDP, SYN/Blade/ACK, and window checking. Attackers start the genuine attack after examining the port.

3.4.6. Man-in-the-Middle Attacks

Man-in-the-middle attacks incorporate an Attackers deliberately obstructing a correspondence between two parties to gain access to the information being sent between them. This attack is made conceivable by a Secure Socket Layer's lack of security configuration (SSL). Now that the two gatherings — including the providers — are associated in the cloud, an Attackers might listen in on the discussion and get the information in the event that the communication routes are not secure.

3.4.7. Attack on Spoofing Metadata

The usefulness and details of the assistance are remembered for the WSDL record. The Attacker's objective in this kind of attack is to gain access to the target record so they might alter or eliminate it. By perusing the record and waiting for service delivery, the attacker effectively stops the service invocation code in the WSDL document. As a component of the guard against this attack, data with respect to support usefulness and different particulars ought to be put away in encoded structure. This kind of record ought to require authentication to get to.

3.4.8. AttackThrough Phishing

A work is made to impact a web connect utilizing phishing. The attack makes a genuine client be shipped off a fake website. The client inputs his data on the open site since he thinks it is secure (username and password). From that point onward, the attacker might get to his credentials.

3.4.9. Attack Through the Backdoor

The backdoor passage channel attack empowers the attackers to get sufficiently close to far off computer programs that deal with the assets of the person in question. It is an unarmed attack. In some cases, a coder will convey zombies with the goal that they can send off a DDoS attack. To control the assets of the victim, nonetheless, attackers habitually use secondary passages channels. It might think twice about information's secrecy and security.

3.5. Security in Data Centres

Cloud systems are similar to group frameworks in that they store and protect hardware. Grid redundancy is crucial to provide a cloud data centre with a robust physical foundation. Cloud service providers ensure that the cloud is highly fault-tolerant, with service efficiency reaching 99.99%. The objectives of cloud service providers include high data availability and reliable services in terms of uptime and flexibility. Each computing server, storage server, and piece of network equipment is securely protected.

The vendor establishes the cost the customers are charged and offers various advanced security options. A Security Operations Centre (SOC) is established to detect suspicious traffic and monitor the network's health. Security Information and Event Management (SIEM) is another approach for achieving elevated levels of network security. SIEM (Security Incident Detection and Mitigation) is a tool used to identify and respond to security incidents. HP ArcSight is an example of a product that performs event correlation.

Data centres employ a four-layered approach, with the foundational level consisting of physical infrastructure, the virtualized computing layer, and the orchestration of virtual infrastructure. Emerging concepts in network connectivity and data storage have introduced security concerns, such as flooding attacks, hardware disruptions, theft, tampering, network abuse, and natural disasters.

4. Conclusion

The development of information technology is now greatly aided by cloud computing. Every cloud consumer continues to demand the best service possible, mainly in terms of security. The lack of standardized norms for the security framework, particularly in the cloud computing community, has becomean unending challenge. Most cloud providers, by default, adhere to best security policies and actively defend the functionality of their systems. Enterprises are required to independently judgethe security of their data, apps, and workloads in the cloud. The complexity of security concerns is increasing as the digital environment develops. Many attacks specifically target cloud computing providers because an organization's complete reliance on data access and mobility makes them an easy target. Although cybersecurity technology is evolving daily, new attack concepts are also emerging regularly. The research will contribute to the development of a resilient security framework, which means that in the event of an attack, rapid detection, segmentation of affected parts of the system (analogous to amputating a part of the body to protect the rest), issue resolution, and subsequent reintegration of the segmented part into the system will enable normal system operation.

References

Abbas, H., Maennel, O., & Assar, S. (2017). Security and privacy issues in cloud computing. *Annals Of Telecommunications*, *72*(5-6), 233-235. https://doi.org/10.1007/s12243-017-0578-3

Ahmed, M., Litchfield, A. T. (2018). Taxonomy for identification of security issues in cloud computing environments. *J Comput Inf Syst*, *58*(1), 79–88.

Bashir, S. F., & Haider, S. (2011, December) Security threats in cloud computing. *Proceedings of the International Conference for Internet Technology and Secured Transactions*, 214–219.

Fan, K., Mao, D., Lu, Z., Wu, J. (2013). OPS: Offline Patching Scheme for the Images Management in a Secure Cloud Environment. InServices Computing (SCC). *2013 IEEE International Conference on Services Computing*. https://doi.org/10.1109/SCC.2013.57

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. *Int J Inf Secur*. *13*(2):113–170. https://doi.org/10.1007/s10207-013-0208-7

Fotiou, N., Machas, A., Polyzos, G. C., & Xylomenos, G. (2015). Access control as a service for the Cloud. *Journal Of Internet Services And Applications*, *6*(1). https://doi.org/10.1186/s13174-015-0026-4

Hubbard, D., & Sutton, M. (2010). Top threats to cloud computing v1.0. Cloud Security Alliance.IEEE International Conference on. Jun 28. IEEE. pp. 587–594.

Kalaichelvi, R., & Arockiam, L. (2015). EnBloAES: A Unified Framework to Preserve Confidentiality of Data in Public Cloud Storage. *Indian Journal Of Science And Technology*, *8*(19). https://doi.org/10.17485/ijst/2015/v8i19/72272

Kaur, M., & Singh, H. (2015). A review of cloud computing security issues. *Int J Adv Eng Technol*, *8*(3), 397–403.

Kavin Prabhu, B., Ganapathy, S., Kanimozhi, U., & Kannan, A. (2020). An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA. *Wireless Personal Communications, 115*(2), 1107-1135.

Khalil, I., Khreishah, A., & Azeem, M. (2014). Cloud Computing Security: A survey. *Computers*, *3*(1), 1-35. https://doi.org/10.3390/computers3010001

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, *125*, 691-697. https://doi.org/10.1016/j.procs.2017.12.089

Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1-48. https://doi.org/10.1016/j.cosrev.2019.05.002

Lee, J. K., Moon, S. Y., & Park, J. H. (2016). CloudRPS: a cloud analysis based enhanced ransomware prevention system. *The Journal Of Supercomputing*, *73*(7), 3065-3084. https://doi.org/10.1007/s11227-016-1825-5

Mell, P., & Grance, T. (2018). SP 800-145, The NIST Definition of cloud computing | CSRC (online) Csrc.nist.gov. Accessed 11 Dec 2018. https://csrc.nist.gov/publications/detail/sp/800-145/final

Naik, N., Jenkins, P., Savage, N., & Yang, L. (2019). Cyberthreat Hunting - Part 2: Tracking Ransomware Threat Actors using Fuzzy Hashing and Fuzzy C-Means Clustering. *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, New Orleans, LA, USA, pp. 1-6. https://doi.org/10.1109/FUZZ-IEEE.2019.8858825

NIST (2011). *The NIST Definition of Cloud Computing*. Accessed September. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

NortonLifeLock Norton Labs. https://www.nortonlifelock.com/blogs/norton-labs/july-2022-consumer-cyber-safety-pulse-report

Oracle.com (2018). The Oracle and KPMG Cloud Threat Report 2018 | Oracle (online). Accessed 11 Dec 2018. https://www.oracle.com/cloud/cloud-threat-report.html

Patil, R., Dudeja, H., & Modi, C. (2019). Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing. *International Journal Of Information Security*, *19*(2), 147-162. https://doi.org/10.1007/s10207-019-00447-w

Pippal, S. K., & Kushwaha, D. S. (2013). A simple, adaptable and efficient heterogeneous multi-tenant database architecture for ad hoc cloud. *Journal Of Cloud Computing*, *2*(1), 5. https://doi.org/10.1186/2192-113x-2-5

Román, R., López, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, *78*, 680-698. https://doi.org/10.1016/j.future.2016.11.009

Ryan, M. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *Journal Of Systems And Software*, *86*(9), 2263-2268. https://doi.org/10.1016/j.jss.2012.12.025

Sgandurra, D., & Lupu, E. (2016). Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems. *ACM Computing Surveys*, *48*(3), 1-38. https://doi.org/10.1145/2856126

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal Of Network And Computer Applications*, *79*, 88-115. https://doi.org/10.1016/j.jnca.2016.11.027

Singh, S., Jeong. Y.-S., & Park, J. H. (2016) A survey on cloud computing security: Issues, threats, and solutions. *Journal Of Network And Computer Applications*, *75*, 200–222. https://doi.org/10.1016/j.jnca.2016.09.002

Singh, J., Refaey, A., & Koilpillai, J. (2020). Adoption of the Software-Defined Perimeter (SDP) Architecture for Infrastructure as a Service. *Canadian Journal Of Electrical And Computer Engineering*, *43*(4), 357-363. https://doi.org/10.1109/cjece.2020.3005316

Soofi, A. A., Khan, M., & Amin, F. (2014). Encryption Techniques for Cloud Data Confidentiality. *International Journal Of Grid And Distributed Computing*, *7*(4), 11-20. https://doi.org/10.14257/ijgdc.2014.7.4.02

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal Of Network And Computer Applications*, *34*(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering*, *71*, 28-42. https://doi.org/10.1016/j.compeleceng.2018.06.006

Sumitra, B., Pethuru, C., & Misbahuddin, M. (2014). A survey of cloud authentication attacks and solution approaches. *Int J Innov Res ComputCommun Eng*, *2*(10), 6245–6253.

Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal Of Network And Computer Applications*, *160*, 102642. https://doi.org/10.1016/j.jnca.2020.102642

Suthar, K., & Patel, J. D. (2017). EncryScation: An Secure Approach for Data Security Using Encryption and Obfuscation Techniques for IaaS and DaaS Services in Cloud Environment. En *Advances in*

intelligent systems and computing (pp. 323-331). Springer, Singapore. https://doi.org/10.1007/978-981-10-2750-5_34

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

Wang, C., Wang, Q., Ren, K., & Lou, W. (2010, Mar). Privacy-preserving public auditing for data storage security in cloud computing. *2010 Proceedings IEEE INFOCOM*. https://doi.org/10.1109/INFCOM.2010.5462173

Wilson, R., & Iftimie, I. (2021). Emerging ransomeware threats: An anticipatory ethical anaylsis. *2021 IEEE International Symposium on Technology and Society (ISTAS)*, Waterloo, ON, Canada, pp. 1-1. https://doi.org/10.1109/ISTAS52410.2021.9629211

Xu, X. (2012). From cloud computing to cloud manufacturing. *Robotics And Computer-Integrated Manufacturing*, *28*(1), 75-86. https://doi.org/10.1016/j.rcim.2011.07.002

Yu, S., Wang, C., Ren, K., & Lou, W. (2010, Mar). Achieving secure, scalable, and fine-grained data access control in cloud computing. *2010 Proceedings IEEE INFOCOM*. https://doi.org/10.1109/INFCOM.2010.5462174

Zhang, Y., Chen, X., Li, J., Wong, D. S., Li, H., & You, I. (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. *Information Sciences*, *379*, 42-61. https://doi.org/10.1016/j.ins.2016.04.015