VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2024, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 12, Number 4, October-December 2024 *pp:167-179*

Protection Issues and Challenges within the Cloud: A Survey

Muhammad Latif [1], **Bushra Mehmood** [1], **Nauman Khalid** [2], **Shahzad Ahmed** [1], **Abdul Basit Abro** [3], **Maaz Ahmed** [1]

[1]Department of Computer Science, Iqra University Faculty of Engineering Science & Technology, Karachi, pakistan. ; [2]Federal Urdu University of Arts, Sciences and Technology.; [3]Department of Computer System Engineering Mehran University,Jamshoro,Pakistan.

Keywords: *Cloud Infrastructure, Software Platform, Computer Protection, cloud security problems*

Journal Info:
Submitted:
November 29, 2024
Accepted:
December 19, 2024
Published:
December 31, 2024

Abstract

A vast range of computing services are accessible over the Internet utilizing the cloud network. In recent years the cloud storage sector and several others have integrated and encouraged scholars to explore emerging technology. Because of its infrastructure and computing capabilities, its device, data, and resources are transferred to the Cloud Storage System. No expensive network infrastructure is required for consumers and their service costs are reduced to a minimum. Regardless of its advantages, the transition of local computing into remote computing has provided customers and vendors with a range of protection issues and threats. The reliable third party provides several cloud platforms that present new security risks. The cloud provider offers its services over the Internet and uses numerous web technologies that create new security challenges. This paper discusses the fundamental features, safety issues, threats, and solutions for cloud information. The paper also discusses many open-ended cloud security research issues. Over the past five years, substantial technological innovations have emerged, which can add extra comfort to daily lives at the corporate and private levels. Both the personal and the shared divisions have significantly progressed in the advancement of cloud storage technologies. It was evident recently that many companies and organizations have transferred the rest of their burdens onto the cloud. However, the protection problem is a significant debate regarding centralized IT control, which is web-based and susceptible to different forms of attacks. While security measures are in place throughout the entire era, security continues to be a challenge. Here we performed a report on distributed computation and investigated various kinds of attacks and dangers on this modern invention, including various kinds of attacks and dangers on the latest concept, combined with protection measures and current structures.

***Correspondence author email address:** abrobasit@gmail.com
DOI: 10.21015/vtse.v12i4.1998

1 Introduction

Across several countries, the breakthrough of cloud storage became commonly adopted and involved the exchanging of information, running programs, and mail. Important CC developments have developed over the last few decades, including considerable progress. The public sector and private sector are generally embraced thanks to the common sense of the CC regimes, which could render things at some stages more feasible. Once again, administrative security is a key issue for both cloud clients and cloud providers [1].

Data protection is a major data safety subdomain and a critical role in the wide usage of cloud technology. As an essential Internet link, the CC services are vulnerable, which may trigger severe attacks and threats to their protection, such as Data Intrusion, Malware Infusions, for searching of Administration Assaults, Knowledge Sadly, and Weak APIs. According to safety incidents in the cloud in the modern age, the number of cloud services has probably increased considerably [2].

More and more enterprises and businesses are shifting their workload to the cloud. As a consequence of the analysis under the guidance of Logic Monitor, a big SaaS management process for IT organizations, by 2020 the number of businesses switching to the cloud would rise by 83% [3].

The implementation of this overall infrastructure will face several problems given advancements in cloud adoption. The security issues in cloud computing continue to be a key issue, as do increased expenditure, lack of resources and expertise, and performance problems, among others, according to Right Scale, the leading cloud computer firm's "cloud status report" [4].

In addition to possible safety features and current results, we carried out a Cloud Computing Survey in this paper to address various types of assaults and security threats against this advancing innovation [5].

In recent years, cloud computing has become a popular business model and one of the fastest-growing IT segments. Hit recessions are rapidly conscious that recessions are quickly accessing best-of-life development technologies through the Web or dramatically improving their network ability. Nevertheless, with the cloud continually providing citizens and businesses with information, environmental conservation issues are growing. This article addresses protection concerns; CSP requirements and risks in the cloud sector. This article addresses topics relevant to protection. For technical and business societies, minimum health and management requirements are developed [6].

There has been continuing worldwide research since the introduction of cloud computing. Cloud computing, the next phase of digital innovation and accelerated IT problems, is viewed as a technological tool. Rapidly increasing cloud computing has raised issues about performance, connectivity, vitalization quality and security, data, public auditing, and scientific use of information systems. Thus, cloud storage has been even more common in recent years. The article attempts to explain emerging CC (Cloud Computing) issues and opportunities. Three times we have examined this paper: first, we analyze the cloud architecture and its different services. We also address some security concerns that concentrate on the cloud storage network layer. However, we consider a variety of transparent subjects and their future consequences in the context of cloud growth. Finally, in the current cloud research and development phase, we highlight the accessible platforms [7].

One of the fastest-changing technologies is cloud storage. Cloud infrastructure has numerous advantages with few protection challenges. This post discusses numerous cloud data privacy concerns and investigates approaches to fix security issues. The article further discusses the implementation and framework capabilities of the cloud network. This is particularly important as data manipulation or abuse infringes people's confidence and may contribute to business loss in any cloud sector or company. In many industries, cloud computing is now used directly or indirectly and would have an impact both on the cloud as well as on the industry should there be data breaches. It is one of the key explanations that data protection is of greater significance in cloud storage

businesses. Data storage and device security are a general environment in which knowledge is guaranteed and access to property, facilities, and stage improvements are guaranteed without restrictions. While the Cloud Infrastructure paradigm provides tremendous benefits, many cloud customers still face protection and functionality problems. This paper offers a thorough overview of safety risk management and security of cloud infrastructure resources. This program would help applicants identify security and security risk factors in a cloud environment in general and would include an exhaustive overview [8].

2 Literature Review

Cloud Computing is a paradigm that provides open, easy network connectivity on request to a typical pool of machine services that can be easily distributed and discharged with no logistical intervention (e.g. networks, servers, data, program, and management cooperation) or partnerships between specialist organizations.

When discussing cloud computing characteristics, this includes functions, structural designs, service models, delivery models, benefits,s, and cloud computing disadvantages. As seen below, the main CC functions. First of all, we'll discuss its self-service on request.

Customers can easily access the self-service program on request through computers like networking, applications, and time for the application. These are scalable systems that do not really need users' help, since consumers have simple access across the Internet to resources they need and are already carrying out the appropriate actions [9].

We will then discuss wide network access. Broad exposure to networking relates to different club capabilities and services which can be accessed widely across the network across several channels (such as computers, cell phones, and tablets). Usually, these cloud systems and infrastructure are situated in a private area inside a business and behind a firewall for fast Internet access from various devices [10].

We should address resource pooling after a large network. Most users utilize a multi-renter approach to share computational power. This strategy encourages consumers to adjust their service levels without physical constraints or even technological services at all times. The consumer is entirely free to usage of such resources, and the consumer might be ignorant of the actual positions of the resources and such utilities are still accessible in the user's mind [10].

The strong elasticity is to be addressed now. Quick versatility for the CC, for example, enables easy scaling (indoors and outdoors) in compliance with customers' requirements in order to easily offer additional cloud capacity at any time for any quantity, and can effortlessly provide a broad variety of resources at a high degree of consistency to consumers at various scales [11].

3 Cloud Computing Architecture

We may address the Cloud infrastructure system during the analysis of this article. This comprises in total of three cloud computing types, the lower layer with the central structure with the remaining layers, the middle layer with the user development and storage system, the top layer with the server one (SaaS), the smallest layer with the key facilities for the other levels, the middle layer with the evolving environment.

3.1 SaaS

SaaS is short for Software as a service. SaaS is often known as an on-demand program that enables users to access software supplied over a cloud platform, including e-mail and remote office suites. Instead of purchasing the latest product, consumers will subscribe for low costs to their company needs for web-based tech services. Security providers are used by customers. SaaS does not provide customers with extraordinary technical equipment but requires a continuous Internet connection. SaaS customers do not have to pay for hardware or software and can conveniently customize their offerings to suit their needs.

3.2 PaaS

PaaS is sort of a platform as a service. PaaS is the second layer that allows engineers to effectively build and execute SaaS systems in PaaS. PaaS entirely

follows the software development cycle and offers entrepreneurs a low-cost solution that does only allows them to handle the underlying infrastructure, but also to build operating apps. Service companies are responsible for the design and operation of building facilities.

3.3 IaaS

LaaS is short of Infrastructure as a service. The lower layer, IaaS, provides the essential architecture for its levels. IaaS covers operating systems, storage, networking, and servers. It helps consumers to access whole properties without the buying of physical products. IaaS often offers a more price-saving and quicker option while operating without the actual agreement needing to be ordered or executed. But, because of Internet access, quality is a key concern.

Deployment Model This essay includes four main models for cloud computing implementation. Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud

3.4 Public Cloud

In a public cloud system, hardware and software assets are freely exchanged by various users. This environment is managed and managed by the public cloud provider of third parties, making these clouds useful for non-responsive data. However, although scalability will never concern public cloud customers, security challenges remain a challenge. The key distinction between public clouds and private clouds is that public cloud customers are not in a position to manage or retain their networks (which is the duty of suppliers) [12].

3.5 Private Cloud

An organization runs a private cloud and only inside this business are all software infrastructure and facilities available. Private clouds are also classified as internal clouds or company clouds. The business is operated by the cloud-based data center and the data is safe behind the firewall. The organization is responsible for both the administration and security of the network. Thus, the private cloud is relatively costly but safe in comparison with the public cloud [13].

3.6 Hybrid Cloud

A hybrid cloud is a combination of two or more types of cloud that is a private cloud. This kind of model provides great flexibility and multiple options for data deployment because it shows the cloud features involved. Central management over a distributed cloud. Depending on needs and resources, the workload can be translated from private to public [14].

3.7 Community Cloud

Community clouds are identical to public clouds in certain ways, although this approach typically includes people, enterprises or organizations with the same cloud specifications. The shared services would be made accessible to participating organizations or third-party service providers on the group cloud.

4 Similar Job

In both academic and market environments, security paradigms are more frequently debated. International workshops focusing on cloud security are conducted at the European Meeting, ACM Cloud Infrastructure Technology Workshop, and Software Safety Strategy International Forum. Several foreign cloud security papers are eligible. This segment includes several survey papers that are our strongest expertise. This report provides a comprehensive study of cloud infrastructure and global security problems. The author concentrates primarily on emerging cloud security problems. The study examines many security concerns, including problems relating to information security, architectural safety, and legal safety and compliance. Nevertheless, this study also found just three aspects of cloud protection problems.

The paper [15] proposed that online providers would be supported with secure security, licensing, and authenticity. The work also addresses areas of mobile cloud storage security. Finally, some open issues are discussed, which were not addressed until now. Specific kinds of cloud security issues have been studied in the paper studies. Each protection concern is separated into layers of the cloud infrastructure and each layer question is analyzed. We look into very short discussions regarding data management and protection problems and approaches in this article.

Safety threats are classified in the paper [16] based on a variety of protection issues. This research includes a review of previous studies. The author

addresses several cloud-related technology issues and presents security problems with each subject. The safety landscape in this document is very broad compared to other documents. This paper essentially provides several recommendations for numerous transparent issues that should in the future be overcome. The suggestions are quite beneficial for potential research work in this area.

The paper [17] discusses the market and implementation paradigm of cloud computing. The author concentrates in particular on the business model and deployment of software systems, including software infrastructure, data storage and protection requirements, in this report. We are still worried about issues regarding cloud computing.

The paper provides an in-depth report on the protection and privacy of providers' cloud services [18]. The speaker describes the concepts of privacy and secrecy separately. First of all, compliance requirements such as anonymity, safety, access management, compatibility, and test software should be given special consideration. The paper offers also a solution for the multi-location data storage system.

An essay [19] gives an overview of the cloud architecture. This tackles different types of cloud assault subsequently. After the attacks were analyzed, a cloud scenario showed the attack detection mechanism and its security. The authors only address cloud overviews, protection, intrusion, and prevention.

The cloud protection of IaaS includes virtualization, computing, networking, and physical measurements. Multi-tenancy is a cloud service that needs to be shared by people and others. Multi-tenancy is the large cloud region that leads to more threats and problems in security. The Cloud Protection Alliance 2010 advice study discusses protection issues and risks.

The paper [20] deals with a framework that deals with health problems related to service distribution models. The authors find the protection function of every distribution type. After the evaluation of the sample authors, a number of problems can be found in the SaaS application model.

The paper [21] gives cloud providers a security environment after identifying many threats and risks in the cloud. Further knowledge of security and safety frameworks is addressed by many cloud storage providers. The report [20] offers a detailed platform-based analysis of security problems relevant to virtualization. The authors first speak about the fundamentals of software simulation and then demonstrate a flexible framework for the virtualization of the computer environment. The research explored the secure separation of networks and identified problems created by heavy virtualization and slow implementation of core virtualization.

The paper [22] focuses on issues with cloud storage and the protection of knowledge. The authors have addressed many concerns, existing challenges, and development in the processing of cloud data and protection. We have analyzed certain web services, authentication and permission issues, availability, and responsibilities issues. They provide remote storage and computation for each feature with such technologies and mechanisms for safe storage and privacy.

A full review of security problems caused by a cloud-based attribute model can be found in the paper [23]. Firstly, the linkages between security features, privacy and the insecurity, threats, and defense techniques of the cloud machine (confidentiality, integrity, anonymity and availability), were addressed.

The article [24] includes comprehensive protection vulnerability assessments in PaaS software infrastructure. The study of the Java and the .NET Isolation Architecture is focused on the multi-tenant paradigm. Article [25] addresses cloud security issues, such as data and outsourced software, sharing of resources, virtualization and overview, convergence, authentication and allowance, identity and access control, trust and stable management of resources, and data storage and privacy. However, the authors send no response. This report also contains no accessible problems.

Cloud technologies and database systems are not specified in paper [26]. The paper discusses safety concerns in e-health clouds specifically. They are also resistant to behavior and transparent queries. Nonetheless, there is so little discussion, only think about safety in the field. Consequently, not all protection issues

are addressed by the privacy strategy. Several cloud-related issues were explored by the writers and protection approaches were then found. Cloud computing technology, structure, model and open-end challenges are not included here.

This research addresses threats and security concerns from the public and private cloud. Following the debate, a number of other issues related to security were resolved, including service quality, multi-tenant service problems, data storage, identity, and access control. They are mainly concerned with data analytics.

5 CLOUD SECURITY

5.1 Cloud safety aspect

It's an aspect of computer security. That specifies a set of information and resources protected strategies, technology,y and controls. The cloud network has direct or indirect effects of threats and aggressions. The protection, efficiency, and openness of cloud providers are breached as are the providers from multiple tiers, and new security problems that occur. The objective of this section is to discuss a variety of security principles to understand cloud security issues.

5.2 Cloud security concepts

Numerous protection problems and risks are protected by cloud computing. The key source of cloud safety hazards and threats is defined in this article. The segment addresses other technology topics such as virtualization, multi-tenancy, digital computing, data sharing, data storage standardization, and security and offers insight into controlled privacy concerns.

- **Virtualized Protection (Computer Virtualization):**
  - Operates in a virtualized IT environment using software-based protection systems.
  - Differs from traditional network security, which relies on static hardware such as firewalls, routers, and switches.
- **Multi-Tenancy in Cloud Storage:**
  - A sharing concept where multiple users (tenants) share a cloud network.
  - Allows co-tenancy, co-location, and co-residential attacks, as sensitive data might be stored in the same physical location.
  - Intruders can exploit shared environments to control adjacent VMs or execute applications.
- **Security Safeguards (Countermeasures):**
  - Measures to reduce or prevent threats and react to risks.
  - Part of a protection strategy that details security precautions and countermeasure information.
  - Includes rules and procedures for safety management to protect confidential information and critical resources.
- **Hostile Agents:**
  - Hostile entities (human or machine) that pose a risk through internal or external attacks.
  - These attacks are particularly dangerous due to administrative rights to access cloud IT services.
- **Defense Systems:**
  - Supported by frameworks for managing computers, confidential data, resources, and knowledge.
  - Defined in terms of countermeasures and guarantees to enhance network safety.
- **Security Policy:**
  - A set of rules and regulations governing security.
  - Explains how laws and policies are implemented in a defense environment.
  - Includes details on the location and use of security checks and procedures.

6 Threats to cloud computing

Danger is defined as something that might significantly damage your computer device. A potential

intrusion on the operating system or network infrastructure may face risks. The paper [23] addressed major threats in conjunction with cloud computing technology architecture.

7 Cloud Protection Threats

Organizations realize the cloud infrastructure value in a client setting. New technologies that formulate fresh cloud assaults were generated day after day. There are certainly different threats as computing utilizes modern web network technologies. Attacks are launched as software utilizes modern computer technologies. In Table 1, a number of safety risks are listed and certain remedies have cloud implications.

8 CLOUD SECURITY ISSUES

This segment will deal with various classified security problems and their solutions. The paper provides a brief overview of cloud computing security issues. Security problems include any threats, errors in design, faults, risks, bugs, and network vulnerabilities. The question in the cloud is somewhat different from the issue in general. The web dilemma is generated and protection strategies become much more challenging to apply in the digital environment due to the characteristics of web machines, as described by NIST. The survey comprises eight secured components: data and system privacy, security issues related to virtualization, internet security issues, network security issues, access management issues, software security issues, trust, enforcement, and legal issues. In the survey, security issues were discussed.

8.1 Collection of data and security processing problems

Data is a core aspect of the cloud. Customer-independent and exclusive data were stored in the cloud. Customers cannot or attempt to risk their data which may have adverse consequences on use or distribution. Your details would also be accurate and reliable to update records at all stages of output. The big issue with centralized or third-party storage is that users are not allowed to retrieve cloud assets until they are restored.

The data owner does not recognize the cloud storage system's location and protection features and computer data safety procedures. The main component of cloud computing is service quality. A cloud storage service requires the best infrastructure and processes to manage cloud data and stability effectively. There are two conditions before and after calculating the results. A variety of protection problems and approaches arising from data management, insecure processing, data and software efficiency, encryption schemes, cloud data recycling, and ransomware are found in Table 2 for the cloud store framework. Analysis needs a system that manages data in the cloud efficiently and safely. Instead, you save the data in a protected location.

8.2 Virtualization Safety Problems

Cloud computing is the most commonly known definition of the virtualized cloud technology market. For business cloud service formation, cloud providers need VM trust. The main demand of any cloud-based business is virtualization. The multi-tenancy and virtualization model produces more advantages but is not free of risks and attacks. Many of the attackers threaten the co-location facilities. In this sector, people routinely work for proper mental and virtual isolation. The virtualization program creates virtualized resources and data and includes many kinds of viruses that can degrade or disable virtualized information. This section discusses thoroughly the protection issue of virtualisation and its approaches. This segment covers a broad variety of security concerns in virtualization, such as VM image management, virtual machine power, network virtualization, compatibility, device problems, and malware, as seen in Table 3.

8.3 Problems connected to the Internet and services

The Cloud Network requires a courier to carry on knowledge from the senders to the receivers in addition to other services and tools. The Web provides a broad range of services via digital data from source to destination. Any nodes move through the data and it is not secure. It is not free. Several new threats

Table 1. Offensive Methods and Their Impacts

No.	Offensive Method	Infrastructure Impacted	Impacts	Result
1	Strike zombie	SaaS, PaaS, IaaS	Availability of resources impacted; may build a false service	Strongly authorship
2	Injection threat operation program	PaaS	Integrity of the company is depressed; malicious services provided instead of legitimate ones	Clear structures of insulation between VMs; Hash feature to track service integrity
3	Virtualization offensive	IaaS	Control passwords of others and monitor	Need a protection hypervisor, track hypervisor operation, and require VM insulation
4	App Threat Client	SaaS	Affects consumer personal details and data protection	Use solid encryption for stronger security
5	Inspection of the port	IaaS, SaaS, PaaS	Company fraud; impacts quality of service	Good protection needed

Table 2. A complete analysis of protection problems and approaches for data collection and computation

No.	Subject of Safety	Safety Problems	Related Articles	Safety Results
1	Space of data	File access central, command failure, pooling in data, position of data, multi-user, complex quality testing layout	[26]	Enhanced citizen data protection
2	Data and quality of resources	Cloud disruption, web device compatibility problem (hardware fault), system disruption	[26]	A data access approach
3	Crystallization	Incorrect cryptography, administrative key malfunctions in cryptography algorithm management	[27]	Encryption to maintain peace; both cloud infrastructure and cryptography
4	Recycling Server Info	Weak execution of technology destruction policies, virtual disk multi-tenant recycle, reused software delete	[28]	Protected deletion of data
5	Virus	Server software replication breakdown, anti-virus failure	[29]	Malware prevention

emerged due to a legacy web 2.0 problem. There are a range of precautions, but people still fear that data shared through the Internet is not secure. The article, described in Table 4, addresses the following issues and explanations.

8.4 Problems linked to network safety

The network primarily consists of cloud services. Problems exist not only in the VM, device, and program processes but also in the network context. Network issues can seriously affect the cloud network. The cloud network is a complex idea that brings both internal and external networks into account. The dynamic architecture and new network development strengthen the basic safety concerns, as seen in Table 5, which can be defined as mobile platforms and security limits.

8.5 Access control issues

Pass control authentication protects against unauthorized reading and writing permissions. Connection security is guaranteed if you authenticate and add an email ID or username and password. Within the multi-tenant computing environment, there are a wide variety of clients. This application uses the cloud infrastructure on platforms through the Front-end GUI. Web technologies or web pages are the gateway to an assault. Therefore, certain methods of access control were required. It is necessary to isolate any element and to enable it logically or physically to solve the question. Table 6 details the access control issues and mitigating solutions.

Table 3. A comprehensive research on compliance problems and approaches for virtualization

No.	Safety Subjects	Safety Problems	Related Articles	Safety Results
1	Control of image VMs	Overlooked image repository, virtual system transience, corrupted virtual computer sprawls, cryptographic overhead due to large-scale VMs, VM image theft, and malicious injections	[28]	A program for VM image processing; Data and quality of VM images
2	Monitoring virtual computers	Hypervisor failure, single point of failure	[29]	Hyper-Check; Hyper-Lock; Split-Visor
3	Mobility	Virtual cloning, virtual replication, online VM relocation, man-in-the-middle replay attack, improper setup	[30]	Security framework for VM migration
4	Issues in virtual machines	Cross-VM attack, covert interface attack, data deduplication challenges, VM data exfiltration attack	[31]	Secure runtime environment
5	Malware	Malware protection failures, malware spreading to metamorphic VM engines	[32]	Unit of protection for intrusion

Table 4. A comprehensive report on protection problems and approaches relevant to Web and Services

No.	Safety Subjects	Safety Problems	Related Articles	Safety Results
1	Repeated and sophisticated threats and toxic creatures	Collection of knowledge, public search, exfiltration of data, cybercrime	[33]	Clear protection regulations; concealed properties
2	Internet protocols	Cryptographic key issues, cookie stealing, cookie poisoning, TLS attacks, impersonation, cookie fraud, confidential contact protocol breaches, network-based multi-tenant attacks	[34]	Using the Cookie Safety Safe Flag
3	Web services	Failed WSDL software review, stateless procedure issues, API transaction integrity, metadata spoofing assaults, insecure WSDL injection records, SOAP wrapping assaults	[34]	XML Encryption Assertions
4	Web technologies	XSS disclosure vulnerabilities, control of compromised websites	[35]	Safety alerts, video monitoring, network access protection, real-time site filtering
5	Connection to Service	Provisioning space	[36]	Database mirroring

8.6 Problems Linked to Program security

The most disturbing problem in today's scenario is machine security. Each software application, that uses a particular programming language, today requires thousands of millions of lines of code. Each system has its ideas. This is why the protective functions of the device cannot be calculated by men. Only when a growing organization observes the law and limits will a mistake counter a security problem. The research evaluated the computational problem in two groups. Third the question of the security of applications and services and third the user interfaces. Table 7 demonstrates the analysis. The table tests include several challenges customer interactions and solutions to accessibility.

9 DISCUSSION AND OPEN ISSUES

The last chapter deals with protection issues linked to the web. It allows the Web not only to be understood by security issues but also by leveraging new software technologies in different forms. At the outset of cloud computing, Internet networks, networks, data security, applications,s, and online infrastructure are standard issues. Owing to multinationals, virtualization, n, and rising pool money, creative protection issues emerge. A cloud storage platform includes multiple devices and services, but the security of services relies on knowledge of resources and value levels. Privacy security in cloud storage, for instance, is more important and challenging to handle as the data owner lacks ownership of the data as moves and processes to the cloud. Often experiments are done in a cloud

Table 5. A comprehensive research on technology issues and approaches for networks

No.	Safety Subjects	Safety Problems	Related Articles	Safety Results
1	Mobilizing networks	Mobile malware extension, backdoor and jailbreaking bugs, rootkits, server access communication bugs, web device vulnerabilities	[36]	Movable interface defense and disruption identification device
2	Protection in circumstances	Remote network access, wide network perimeter, DMZ presumption, firewalls limitation, restricted VMM networking link, spoofing of security risks, inadequate method of surveillance	[37]	Digital computer network and software network

Table 6. A comprehensive analysis of challenges and approaches relevant to access management

No.	Safety Subjects	Safety Problems	Related Articles	Safety Results
1	Connection to physical	Malicious outsiders, hot boot assault, balanced hardware, malicious device admin	[37]	Express Access rules, Protect access to data, Using extensible language access management markup (XACML)
2	Permission to use	Inapplicability of data mashups on centrally accessed managed malicious software, insufficient or incorrect assignment of authorization, URL divination assault	[38]	Connection management dependent on responsibilities

system to address protection problems. In fact, a variety of open problems remain essential to address a secure cloud infrastructure. A comprehensive and optimized mitigation approach that satisfies all of the main cloud safety criteria would be the first and most important open issue. Every researcher works on a particular security problem and fixes it by himself. Analysis and problem-solving can contribute to other protection approaches to a particular issue. In a real case, a particular question cannot be overcome by several protection approaches. Using and handling many technology systems alone may be dangerous. An increasing and streamlined protection approach is simpler and easier to enforce with technology software. Multi-tenancy provides a multi-user data-sharing cloud storage system. New protection risks are raised by the cloud computing network. Data encryption and privacy are also some of the security problems that are most available. Health and secrecy. The research in this area provides a variety of approaches, but not all the issues are solved with the approach. The machine resource pool model provides a dependable access control scheme. Unauthorized access to cloud service is restricted by the access management program. The dynamic distribution of capital makes the complexity of services more complex. A

Table 7. Security Topics and Solutions in Platforms, System Frameworks, and Client-side Concerns

No.	Security Topic	Security Issues	Studies	Security Solution
1	Platforms and system frameworks	Uncertain device calls and poor memory insulation, poor SDLC systems used for insulation between devices, secure thread termination, resource management	[39]	Privacy multi-locator mobile framework
2	Front of Client	Device visibility, imperfect setup	[40]	Detection of lightweight interference, Malware Management

problem in the cloud is user identification and security management. The transformation of client identity to cloud-based identity and the pace of adjustment in this phase is a significant factors in assessing the performance of the cloud program.

10 CONCLUSION

Cloud Storage offers quick distribution, affordable costs, vast capability, and easy device connectivity all over the world. Thus, cloud computing is very evident and is widely utilized worldwide. Many protection and privacy concerns often impede the usage of cloud storage. The errors, hazards, and cyber threats are well-known by all cloud customers. Knowing technology flaws and threats would enable organizations to easily access the cloud. The fusion of new and modern technology is used in cloud computing. These new technologies will contribute to various problems with cloud security. The multi-tenancy and cloud virtualization capability helps people to use the same physical infrastructure from multiple locations. The inadequate separation between VMs would harm the protection of the device. Throughout this paper, we addressed the core aspects of cloud storage and safety concerns that arise from the cloud being virtualized, centralized, shared, and public. The paper also proposed numerous countermeasures to fix cloud protection concerns in many fields. The table listing health accidents, risks, problem,s, and their remedies can be of great help to writers. The conclusion of the paper will encourage scientists to focus on open issues inside the field.

Author Contributions

Muhammad Latif: Conceptualization, Methodology, Software.**Bushra Mehmood**: Data curation, Writing - Original draft preparation.**Nauman Khalid**: Visualization, Investigation. **Shahzad Ahmed**: Software, Validation.**Abdul Basit Abro** (Corresponding Author): Supervision. **Maaz Ahmed**: Writing - Reviewing and Editing.

Compliance with Ethical Standards

It is declared that all authors don't have any conflict of interest. It is also declared that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

Funding Information

FMS acknowledges the support of NSF grant CHE-1111111.

References

[1] L. Alhenaki, A. Alwatban, B. Alahmri, and N. Alarifi, "Security in cloud computing: A survey," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 4, 2019.

[2] A. Elzamly, N. Messabia, M. Doheir, S. Abu Naser, and H. A. Elbaz, "Critical cloud computing risks for banking organizations: Issues and challenges," *Religación. Revista de Ciencias Sociales y Humanidades*, vol. 4, no. 18, pp. 673–682, 2019.

[3] Y. W. Chang, "What drives organizations to switch to cloud erp systems? the impacts of enablers and inhibitors," *Journal of Enterprise Information Management*, vol. 33, no. 3, pp. 600–626, 2020.

[4] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, and H. Arshad, "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers & Security*, vol. 112, p. 102494, 2022.

[5] C. S. Lai, Y. Jia, Z. Dong, D. Wang, Y. Tao, Q. H. Lai, and L. L. Lai, "A review of technical standards for smart cities," *Clean Technologies*, vol. 2, no. 3, pp. 290–310, 2020.

[6] C. Bonina, K. Koskinen, B. Eaton, and A. Gawer, "Digital platforms for development: Foundations and research agenda," *Information Systems Journal*, vol. 31, no. 6, pp. 869–902, 2021.

[7] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *The journal of supercomputing*, vol. 76, no. 12, pp. 9493–9532, 2020.

[8] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682–4696, 2020.

[9] W. J. Ali, A. Q. A. Latif, M. Y. M. Ali, I. Ali, M. Ebrahim, and A. A. Abro, "Auctisafe: Building a robust and reliable auction system for optimized security measures," pp. 1–6, 2024.

[10] D. J. Schaeffer, L. M. Klassen, Y. Hori, X. Tian, D. Szczupak, C. C. C. Yen, and A. C. Silva, "An open access resource for functional brain connectivity from fully awake marmosets," *NeuroImage*, vol. 252, p. 119030, 2022.

[11] M. Ghasemaghaei, "Understanding the impact of big data on firm performance: The necessity of conceptually differentiating among big data characteristics," *International Journal of Information Management*, vol. 57, p. 102055, 2021.

[12] A. Hassan, M. Ebrahim, A. A. Abro, K. Raza, and S. H. Adil, "Criisl: Convert rasterize image into svg layers," *The Asian Bulletin of Big Data Management*, vol. 4, no. 1, pp. Science–4, 2024.

[13] I. Ali, S. H. Rizvi, S. H. Adil, and A. A. Abro, "Code smell detection and software refactoring research: A systematic literature review," *The Asian Bulletin of Big Data Management*, vol. 4, no. 1, pp. Science–4, 2024.

[14] L. Gastearena-Balda, A. Ollo-López, and M. Larraza-Kintana, "Are public employees more satisfied than private ones? the mediating role of job demands and job resources," *Management Research: Journal of the Iberoamerican Academy of Management*, vol. 19, no. 3/4, pp. 231–258, 2021.

[15] M. Jangjou and M. K. Sohrabi, "A comprehensive survey on security challenges in different network layers in cloud computing," *Archives of Computational Methods in Engineering*, vol. 29, no. 6, pp. 3587–3608, 2022.

[16] S. M. Daniyal, S. M. T. Hussain, F. L. Abbasi, D. Hussain, M. M. Abbasi, and U. Amjad, "A hybrid deep learning model for precise epilepsy detection and seizure prediction," *Spectrum of engineering sciences*, vol. 2, no. 3, pp. 62–77, 2024.

[17] W. Saeed and C. Omlin, "Explainable ai (xai): A systematic meta-survey of current challenges and future opportunities," *Knowledge-Based Systems*, vol. 263, p. 110273, 2023.

[18] M. Saleem, M. Haris, M. Naeem, A. B. Abro, M. Ahmad, and A. Ahad, "A blockchain-powered loan management system enhanced with smart contract," pp. 1–5, 2024.

[19] M. Chauhan and S. Shiaeles, "An analysis of cloud security frameworks, problems and proposed solutions," *Network*, vol. 3, no. 3, pp. 422–450, 2023.

[20] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro, and T. F. Pena, "Security by design for big data frameworks over cloud computing," *IEEE Transactions on Engineering Management*, vol. 69, no. 6, pp. 3676–3693, 2021.

[21] S. El Kafhali, I. El Mir, and M. Hanini, "Security threats, defense mechanisms, challenges, and future directions in cloud computing," *Archives of Computational Methods in Engineering*, vol. 29, no. 1, pp. 223–246, 2022.

[22] M. L. L. Miguel and F. Marques, "A real application of multi-tenancy in an alarm system software," Master's thesis, Universidade de Coimbra (Portugal), 2023.

[23] Z. B. Akhtar, *Securing operating systems (OS): a comprehensive approach to security with best practices and techniques*, 2024.

[24] J. B. Decourcelle, T. D. Ngoc, B. Teabe, and D. Hagimont, "Fast vm replication on heterogeneous hypervisors for robust fault tolerance," in *Proceedings of the 24th International Middleware Conference*, 2023, pp. 15–28.

[25] J. Sung, S. J. Han, and J. W. Kim, "Cloning-based virtual machine pre-provisioning for resource-constrained edge cloud server," *Cluster Computing*, vol. 27.

[26] S. M. Daniyal, A. Masood, M. Ebrahim, S. H. Adil, and K. Raza, "An improved face recognition method based on convolutional neural network," *Journal of Independent Studies and Research Computing*, vol. 22, no. 1, pp. 103–110, 2024.

[27] S. M. Daniyal, M. M. Abbasi, D. Hussain, U. Amjad, A. B. Abro, and M. Naeem, "A hybrid approach for simultaneous effective automobile navigation with de and pso," *VAWKUM Transactions on Computer Sciences*, vol. 12, no. 2, pp. 01–15, 2024.

[28] M. M. Abbasi, S. M. Daniyal, A. A. Abro, D. Hussain, U. Amjad, and N. B. Zahid, "Applying neural networks to predict ventilator demand: A study of pakistan's healthcare sector," *VFAST Transactions on Software Engineering*, vol. 12, no. 3, pp. 217–229, 2024.

[29] M. S. H. Talpur, A. A. Abro, M. Ebrahim, I. A. Kandhro, S. Manickam, S. U. Arfeen, A. Dandoush, and M. Uddin, "Illuminating healthcare management: A comprehensive review of iot-enabled chronic disease monitoring," *IEEE Access*, 2024.

[30] W. A. Siddique, M. F. Siddiqui, A. K. Jumani, W. Hyder, and A. A. Abro, "Big data analytics for 6g-enabled massive internet of things," in *Low-Power Wide Area Network for Large Scale Internet of Things*. CRC Press, pp. 177–202.

[31] M. Latif, M. Ebrahim, A. S. Abro, M. Ahmed, M. D. Abbasi, and I. A. Tunio, "Face recognition from video by matching images using deep learning-based models," *VAWKUM Transactions on Computer Sciences*, vol. 12, no. 2, pp. 50–64, 2024.

[32] A. Arshad, S. H. Adil, and M. Ebrahim, "Plant disease detection using convolutional neural network," *Journal of Independent Studies and Research Computing*, vol. 22, no. 1, pp. 73–79, 2024.

[33] A. A. Khan, A. A. Laghari, A. Kumar, Z. A. Shaikh, U. Baig, and A. A. Abro, "Cloud forensics-enabled chain of custody: a novel and secure modular architecture using blockchain hyperledger sawtooth," *International Journal of Electronic Security and Digital Forensics*, vol. 15, no. 4, pp. 413–423, 2023.

[34] A. U. Nabi, M. Ahmed, and A. Abro, "An overview of firewall types, technologies, and functionalities," *International Journal of Computing and Related Technologies*, vol. 3, no. 1, pp. 10–16, 2022.

[35] V. Raja *et al.*, "Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns," *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, vol. 4, no. 1, pp. 121–144, 2024.

[36] A. K. Y. Yanamala, "Emerging challenges in cloud computing security: A comprehensive review," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 4, pp. 448–479, 2024.

[37] H. K. Mistry, C. Mavani, A. Goswami, and R. Patel, "The impact of cloud computing and ai on industry dynamics and competition," *Educational Administration: Theory and Practice*, vol. 30, no. 7, pp. 797–804, 2024.

[38] S. Ali, S. A. Wadho, A. Yichiet, M. L. Gan, and C. K. Lee, "Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing," *Egyptian Informatics Journal*, vol. 27, p. 100519, 2024.

[39] A. Mughaid, I. Obeidat, L. Abualigah, S. Alzubi, M. S. Daoud, and H. Migdady, "Intelligent cybersecurity approach for data protection in cloud computing based internet of things," *International Journal of Information Security*, vol. 23, no. 3, pp. 2123–2137, 2024.

[40] V. K. Kasula, A. R. Yadulla, B. Konda, and M. Yenugula, "Fortifying cloud environments against data breaches: A novel ai-driven security framework," 2024.