

Security in Cloud Computing: Issues and Challenges

¹Dr. Mohammad Ahmar Khan, ²Dr. Pratibha Gupta, ³Abdulsatar Abduljabbar Sultan, ⁴Dr. Preeti Singh, ⁵Shivam, ⁶Dr. Melanie Lourens

Submitted: 21/12/2023 Revised: 27/01/2024 Accepted: 09/02/2024

Abstract: Cloud computing is a popular social phenomena that most people use on a regular basis. There are some themes that are universally accepted, much like at any big social event. In the current context, cloud computing is viewed as a quickly evolving field that, with the aid of hardware and software virtualization, may instantly provide extensible services via the Internet. The ability to lease and release resources on a flexible basis in accordance with user requirements is the largest benefit of cloud computing. Additional advantages include increased efficiency, which balances operating costs. This lowers the expensive price of software and hardware. Adopting the newest cloud technology has numerous advantages, but there are privacy concerns as well because data on the cloud might move from provider to provider at any time.

The past few decades have seen a steady increase in demand, which has resulted in a notable rise in interest in cloud computing. Organisations using cloud-based data storage solutions may benefit from a number of factors. These include the potential financial benefits from cloud computing, simpler IT infrastructure administration, and remote information access from any location in the globe with a stable Internet connection. Further research is needed to fully understand the security and privacy issues related to cloud computing. In earlier investigations, researchers from standards organisations, academia, and industry have suggested possible remedies for these problems.

Most issues stem from the fact that the consumer no longer has control over their data because it is stored on a single machine that is owned by the cloud provider. Because their interests may differ (the user may wish his information to be kept private, but the owner may desire to utilise this for his own company), this happens when the owner of the remote server is a different person or organisation than the user. Concerns regarding automated management, guaranteed IoS provisioning, and uncertainty about future cloud system upgrades further impede the adoption of cloud technology. This study covered the fundamentals of cloud computing as well as security flaws, vulnerabilities, and fixes. The article also discusses a number of important cloud-related subjects, including cloud technologies, cloud architectural frameworks, and cloud security ideas, risks, and threats.

Keywords: Cloud computing, Internet, Hardware, Software, Technology

1. Introduction

"Cloud computing" refers to both the technology and software found in the datacenters that host the Internet-based programmes that are offered as services as well as the applications themselves. The growth of the internet and computing resources has made the evolution of technological knowledge more powerful and dominant than it has ever been. A new computer prototype known as cloud computing has arisen as a result of technology becoming more broadly available and affordable. Clouds

are sizable pools (or clusters) of operationally available virtualized resources, including platforms, development services, and hardware, that may be dynamically modified to provide the best possible resource utilisation in terms of load balancing, elasticity, and scalability. In contrast to conventional approaches, cloud computing offers scalability and makes it possible to provide a service entity's compressed form to several customers at a reasonable price. To accommodate consumer needs for communication, storage, and processing capacity, numerous firms, including Microsoft, Google, and Amazon, have created large data centres throughout the world to serve as their public clouds.

In order to provide on-demand services over the Internet, cloud computing makes extensive use of virtual storage. The main advantages of cloud computing are that it eliminates the need for the customer to set up an expensive computer infrastructure and offers low-cost services. In recent years, cloud computing has become more intertwined with many different facets of the economy, which has prompted researchers to investigate new related technologies. Because cloud storage servers offer services that are easily accessible and scalable for computing operations, people and businesses are migrating their

¹Associate Professor, Department of MIS, College of Commerce and Business Administration, Dhofar University, mkhan@du.edu.om

²Assistant Professor, Faculty of Management & Commerce, Poornima University, Jaipur. e-mail ID: pratibha.gupta@poornima.edu.in. ORCID ID: 0009 0000 5812 4506

³Business Management Department, Catholic University in Erbil. Abdulsatar.sultan@cue.edu.krd

⁴Associate Professor, School of Media, Film and Entertainment, Sharda University, Uttar Pradesh. preetisingh.jmc@gmail.com

⁵Assistant Professor, Department of Computer Science & Engineering, MM Engineering College, Maharishi Markandeshwar (Deemed to be University), Mullana-Ambala, Haryana, India 133207. shivamrana41@gmail.com

⁶Deputy Dean Faculty of Management Sciences, Durban University of Technology, South Africa. Email: melaniel@du.ac.za. Orcid: 0000-0002-4288-8277

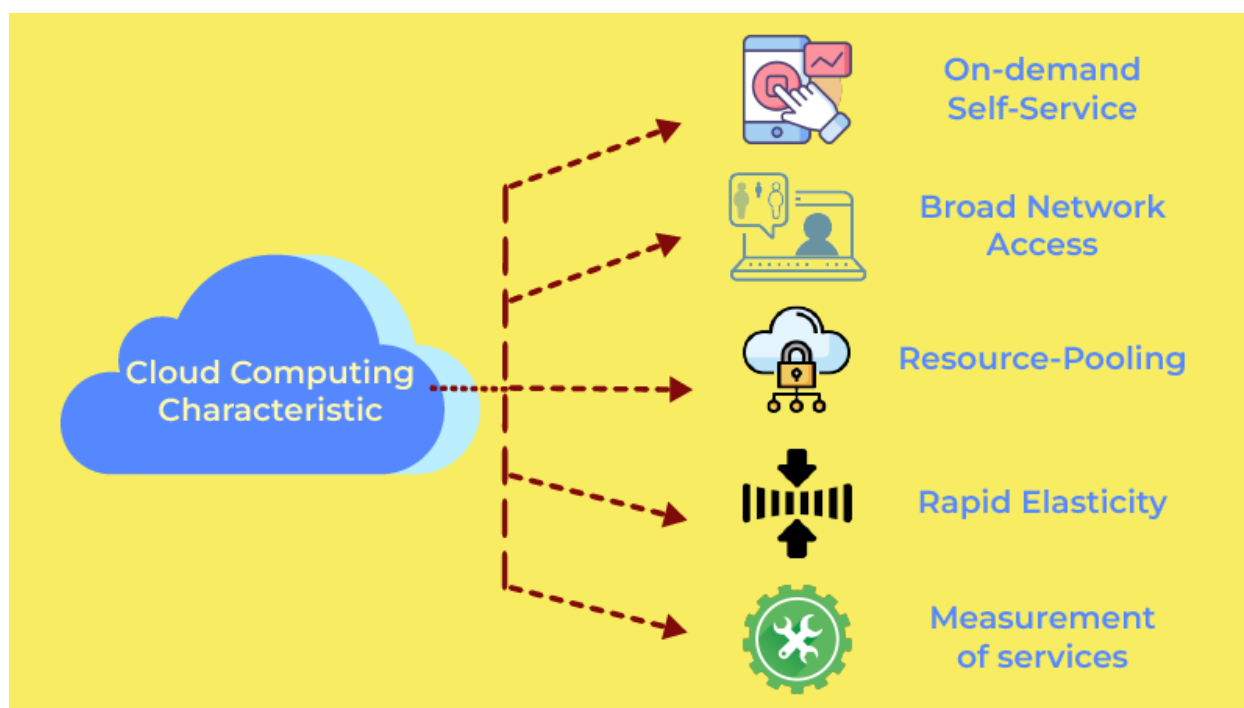
apps, data, and services to these servers. Despite the advantages, there are a number of security risks and challenges associated with the move from local to remote computing for both service providers and clients. There are now more security threats because many cloud services are provided by a reputable third party.

We never consider how electricity is produced or enters a channel when we plug in any kind of electrical appliance. This phenomenon can occur due to the virtualization of power. This power is accessible through a wall outlet, but the massive dispersed grid and power generating facility are hidden. Researchers who increase the usage of information technology by offering useful information and services that users are unaware of can build on this concept. The computational environment is thought to be fully virtualized.

The majority of big and small IT organisations used traditional methods—that is, they needed a separate server room—to store their data before utilising cloud computing. There ought to be a mail server, firewall, router, modem, high-speed internet equipment, and a database server in the server room. IT organisations have to invest a lot of money in that. Cloud computing emerged as a solution to all of the cost issues, and the majority of businesses now use this technology.

2. Characteristics of Cloud Computing

Many characteristics make cloud computing one of the sectors with the quickest rate of growth in the modern economy.



Source: <https://medium.com/@gevbimtek>

2.1 Resources pooling: Resource pooling is one of the key components of cloud computing. The capacity of a cloud service provider to distribute resources across several clients while still offering each one a special set of services catered to their requirements is known as resource pooling. It is a multi-client method that can be applied to processing, bandwidth provisioning, and data storage. The administration approach for real-time resource allocation does not interfere with the client's experience.

2.2 On-demand self-service: It's one of the most important and crucial aspects of cloud computing. It gives the client the ability to keep an eye on the server's capabilities, uptime, and accessible network storage. This

is a basic feature of cloud computing, where the user sets the processing power according to his need.

2.3 Easy maintenance: One of the best things about clouds is this. The servers are simple to maintain, and there is very little, if any, downtime. Resources based on cloud computing undergo constant updates to enhance their capabilities. The upgrades work faster than previous iterations and are more device-compatible.

2.4 Scalability and rapid elasticity: One important aspect and advantage of cloud computing is its rapid scalability. With the help of this cloud function, workloads that require a lot of servers can be operated affordably for brief periods of time. Such workloads are common among clients, and because of cloud computing's

rapid scalability, they can be managed relatively economically.

2.5 Economical: This cloud feature helps businesses cut down on their IT spending. For the cloud computing space they have utilised, the client is responsible for paying the administration. There aren't any extra costs or hidden fees to pay. Because of their thrift, the administration regularly gives away some space.

2.6 Measured and reporting service: Reporting services are only one of the many advantages that make the cloud the best choice for companies. A reporting and measuring system helps cloud providers and their customers. It enables reporting on the services used and for what purposes by both the client and the service provider. This facilitates managing billing and maximising the usage of resources.

2.7 Security: Data security is one of the best aspects of cloud computing. Cloud services create a copy of the data in order to prevent data loss. The duplicate copy from the other server can be used to restore the data in the event that one server loses it. This feature is useful when multiple people are working on a single file at the same time and the file becomes corrupted.

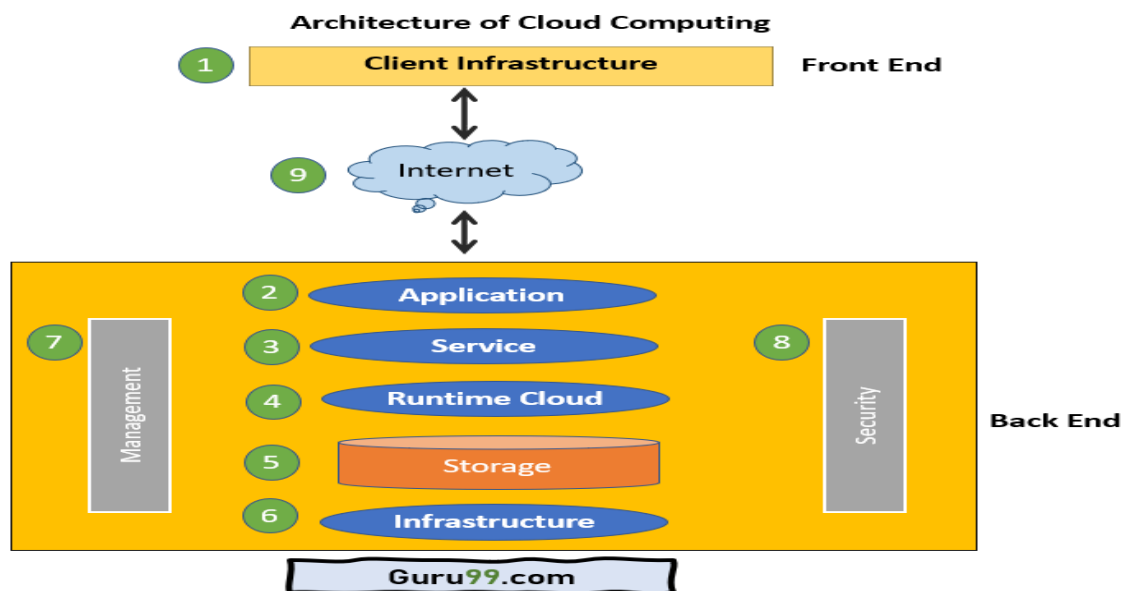
2.8 Automation: Cloud computing is special because it automates tasks. Automation is the capacity of cloud computing to set up, install, and maintain a cloud service

automatically. In short, it's the practice of maximising technology while minimising physical exertion. However, it is more difficult to achieve automation in a cloud setting. Servers, virtual machines, and a lot of storage must be installed and made operational. These resources will need regular maintenance after they have been deployed appropriately.

2.9 Resilience: Resilience in cloud computing refers to a service's ability to quickly bounce back from an interruption. One important measure of a cloud's resilience is how quickly hacked servers, databases, and network services restart and recover. The accessibility of cloud computing is another crucial component. Because cloud services may be accessed from anywhere, there are no geographical limitations or limits when it comes to employing cloud resources.

2.10 Large network access: The broad use of the cloud is one of its most unique features. All the client needs is a device and an internet connection to access cloud data or send data to the cloud from any location. Throughout the entire organisation, these abilities are accessible through these online tools. Cloud providers save a tonne of network traffic by monitoring and guaranteeing a number of factors, such as latency, access time, and data throughput, which show how customers use cloud services and data.

3. Cloud Computing Architecture



Source: <https://www.guru99.com/>

The design of cloud computing offers scalability for processing large amounts of data in a tenant organisation. Specific characteristics like resource pooling, self-service, measurement services, and wide network access might improve a cloud architecture. SOA (Service Oriented

Architecture) and EDA (Enterprise Data Architecture) (Event Driven Architecture) are combined in cloud computing architecture. The architecture of cloud computing consists of runtime, storage, infrastructure,

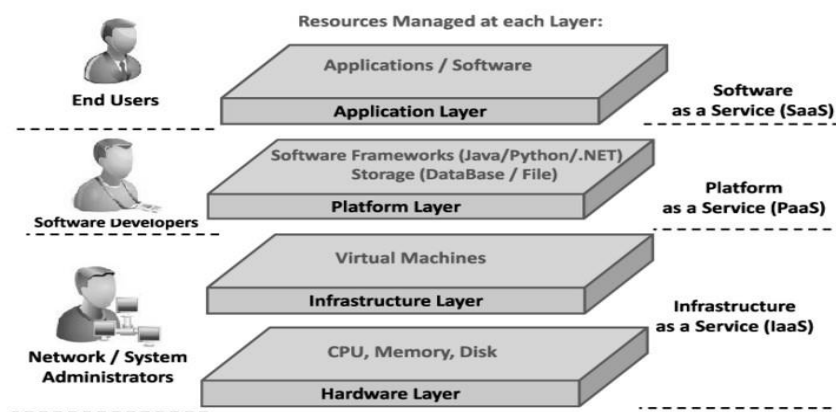
management, and security in addition to client infrastructure and applications.

A frontend architecture is one that the client or user can see. Client-side interfaces and applications necessary for utilising cloud computing platforms are included. A network, like the Internet, is used for communication between the frontend and backend. Additionally, the middleware enables the frontend to send queries to the backend. Examples include web servers, tablets, smartphones, and various client sizes.

The backend, on the other hand, refers to the cloud. It is a group of tools used by cloud computing providers (sometimes called hosts) to administer and operate cloud services. Users' data is safeguarded by it. Middleware, which enables device connectivity and communication, is also included in the backend.

The frontend's data is protected by the backend, which also provides prompt customer service. In addition to security, traffic management is covered in this aspect of cloud architecture design. For instance, traffic control systems, virtual machines, big data storage, etc.

4. Components of the Cloud Architecture



Source: <https://websiteton.com/>

4.1 Frontend of Cloud Computing Architecture: All of the user interface's interactions are shown on the cloud computing architecture's front end. A user interface is made up of several subcomponents that work together. The User Interface, Client Infrastructure, Software, and Network are the main frontend components.

4.2 Backend of Cloud Computing Architecture: The backend facilitates the functionality of the frontend. It is composed of storage and hardware. The Cloud Computing backend is fully under the control of a cloud service provider. Reliability is critical to the backend of the cloud architecture since it holds everything together. The application, runtime cloud, storage, infrastructure, management software, and security are the main parts of the backend architecture.

5. Objectives of the Study

5.1. Identify the security issues that cloud computing is currently facing and the literature's remedies.

5.2. Analyze the difficulties for which there are no established mitigation techniques.

6. Research Question

6.1. What security-related issues exist in cloud computing?

6.2. What remedies are available to address cloud security-related issues?

6.3. How does a company address a security issue that has been identified but for which there are no plans for mitigation?

7. Methodology and Results

The suggested framework protects data against the system administrator who has the highest authority on a storage node. Every storage node in the system is equipped with a Trusted Platform Module (TPM) chip, which provides remote attestation of every storage node and secure storage of encryption/decryption keys for client data. The TPM holds the corresponding keys, and each storage server includes an encrypted file system that encrypts the client's data. Cryptographic techniques are employed to provide secure communication between the client and the cloud. The system guarantees that the client's data is only stored on reliable storage servers and that hostile system administrators cannot transfer it to a corrupt node.

7.1 Implementation Design

A cloud computing platform sent on at least one host with at least one hardware TPM chip for each figure host and network connectivity between the hosts are crucial

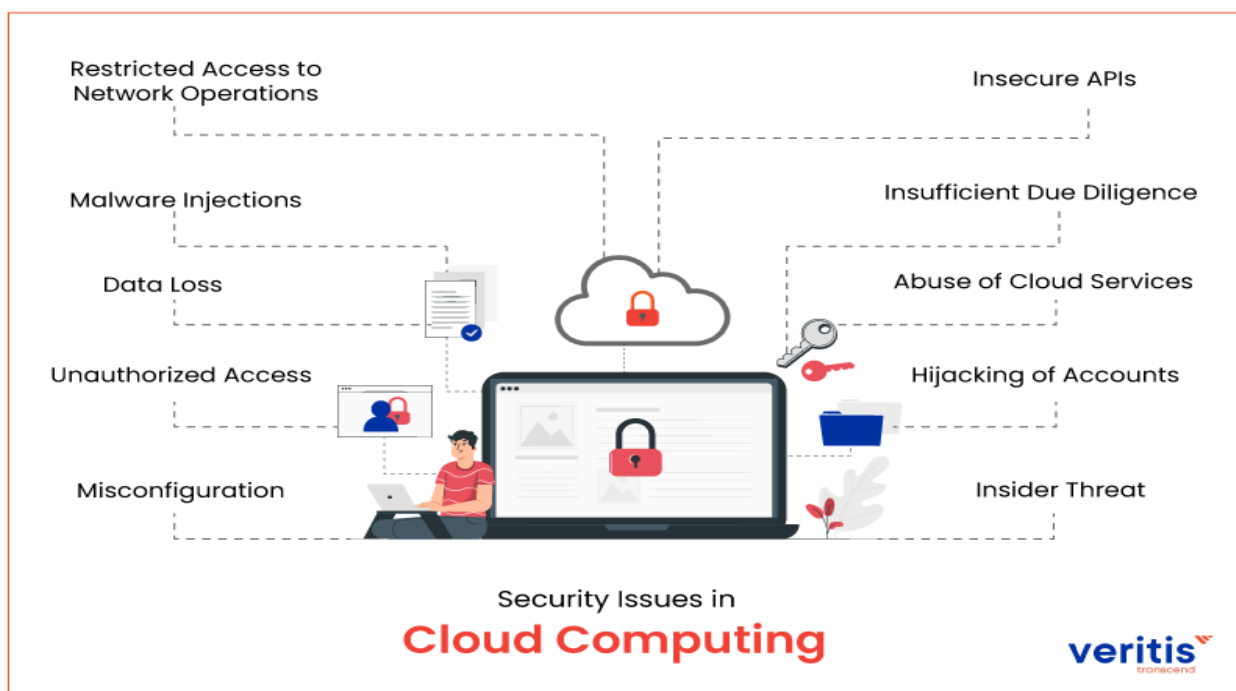
components for the implementation of the aforesaid convention. Two physical servers were used in the current implementation; one host operated an OpenStack Compute service, while the second host handled the other necessary OpenStack services as well as the Trusted Third Party service. Over a Cat6 link, a steered Ethernet connection was used to establish communication between the nodes.

7.2 Controller node setup

A Dell OptiPlex 170L with an Intel(R) Pentium(R) 4 CPU 2.80GHz processor and 1 GB RAM served as the cloud controller's host.

7.3 Compute node setup

8. Issues in cloud computing



Source: <https://www.veritis.com/>

Undoubtedly, cloud computing offers a multitude of benefits; yet, it also presents certain security risks. The security issues with cloud computing are listed below. The multi-tenancy aspect of cloud computing makes cloud adoption more difficult.

8.1. Privacy: The host company may choose to access user information with or without permission. The data kept on the cloud is constantly accessible to the service provider. They might willfully change, remove, or even modify data.

8.2. Compliance: Different kinds of hosting and data are needed in different places. The user may need to adopt pricey deployment procedures in order to comply with requirements (such as the Federal Information Security

A Dell PowerEdge 310 with an Intel(R) Xeon(R) CPUX3450, 2.67GHz, and 8 GB of RAM served as the process node's host. The host had a TPM chip 1.2 Level 2 installed.

7.4 Implementation of TPMI

The following ancillary public services were discovered by the TPMI to support the proposed convention:

Calling Attest host/2 from manager.py is necessary to verify the host and obtain the N^0 , H_{VM}

Initiate_attestation (URL :: string ()),

Token :: string ()

Management Act, the Health Insurance Portability and Accountability Act, and others).

8.3. Security: Cloud-based services make use of third-party security and storage. If someone uses a cloud-based company for free or at a reduced rate, is it reasonable to expect them to safeguard and preserve their data? They are able to divulge user data to third parties. Threats to security can arise from the cloud.

8.4. Sustainability: The location of the servers in relation to cloud computing might have a variety of environmental effects. Some areas have easy access to renewable energy sources and natural cooling, with no environmental effects. A little decrease in energy use could lead to a large reduction in carbon footprint because data centres are

located in dispersed clouds and have access to a variety of energy sources, including renewable energy.

8.5. Abuse: In addition to purchasing hardware for personal use, a consumer may purchase cloud computing services to be used maliciously. This includes starting attacks and breaking passwords using the premium services.

8.6. Higher Cost: A normal cloud service subscription won't cut it if your business is large and diversified. To utilise cloud services uninterrupted, you'll need a strong network with higher capacity than standard internet networks. Otherwise, it could be inconvenient to work on complex projects and apps while utilising a regular cloud service. This is a significant problem that keeps small firms from implementing cloud computing into their daily operations.

8.7. Recovery of lost data in contingency: Examine all policies and documentation from cloud service providers before signing up with one to make sure their offerings fit your demands and that they have a sufficient infrastructure of resources that need regular maintenance. If you sign up for the service, you virtually provide your data to a third party. The fear of recovering lost data in the future can be eliminated if you choose the correct cloud service.

8.8. IT management: A suitable and necessary IT governance model is needed for cloud computing in order to maintain a secure computing environment that conforms with all applicable corporate IT and legal requirements. A number of organisational competencies are necessary for the effective deployment and upkeep of cloud services, including demand management, relationship management, data security management, risk, and compliance management.

8.9. Lack of resources/skilled expertise: A basic issue facing today's companies and organisations is a shortage of qualified personnel and resources. It seems like every other company is either considering cloud services or has already shifted to them. Because of this, cloud service hosting providers must continue to innovate quickly in order to meet the expanding workload in the cloud. These factors are making it tough for organisations to stay up to date with the tools. With new tools and technologies emerging every day, there is a constant need for more experienced and trained personnel. The only way to lessen these challenges is to give IT and development staff further training.

9. Challenges in Cloud Computing

9.1 Adequate Protection: Due to the novelty of cloud computing and its increasing adoption by startups, it attracts hackers who wish to deliberately breach networks

and steal confidential information. Security of the data is one of the main issues. Phishing, botnets, and data loss are all major security risks for the software and data inside an organisation.

9.2 Passwords Security: Your cloud account gets increasingly insecure the more users have access to it. Anyone who has access to your cloud account or knows your password will be able to view your personal data. In this situation, the company needs to make sure that credentials are secure and employ multi-level authentication. Regular password changes are also necessary, particularly once an employee quits or departs the organisation. Passwords and usernames should only be distributed very seldom.

9.3 Cost of Cloud Computing: By accessing application software via a fast internet connection and cloud computing, you can reduce the cost of computer hardware, software, management, and maintenance. The cost is decreased as a result. But it's expensive and challenging to modify the organization's requirements on a third-party platform.

9.4 Lack of Expertise: As workloads have increased and cloud technologies have evolved, cloud technology management has become more complex. There has long been a need for a skilled labour force that can operate with the tools and services of cloud computing. Therefore, companies need to train their IT staff to reduce this risk.

9.5 Control: An additional ethical concern with cloud computing is maintaining appropriate control over asset management and upkeep. It is the responsibility of a committed team to ensure that the resources utilised to deliver cloud services are utilised in compliance with established policies and guidelines. Assets should be used efficiently, and maintenance should be performed when needed, in order to achieve your company's objectives.

9.6 Performance: Your business depends on your supplier when you move your corporate programmes to the cloud or to a third-party vendor. Selecting the right cloud service provider is one of the biggest challenges in cloud computing.

Look for companies that use cutting edge technologies before making an investment. The functionality of BIs and other cloud-based systems is also integrated into the provider's systems. Be cautious when selecting a provider, and confirm that they have procedures in place to address issues as soon as they arise.

9.7 Multiple Cloud Management: Businesses are starting to invest in hybrid clouds, several private clouds, or a large number of public clouds. The popularity of this has surged in the last several years. Because of this, it's now essential to recognise the problems that these

companies face and provide solutions in order to stay ahead of the curve.

10. Conclusion

This paper outlines the broad security risks associated with cloud computing as well as the mitigating strategies that have been suggested to address those issues. However, there are still some issues that lack solutions, which could worry and pose a risk to some ardent fans of CC.

Ultimately, we think that cloud computing offers an excellent platform for companies to develop and prosper. However, when adopting one, you have to proceed with caution. Make a thoughtful selection regarding your supplier, taking into account their compliance standards and the existence of a risk and weakness management plan. Cloud computing has bright possibilities for researchers and enterprises alike, but there are a lot of difficult issues to resolve, including security, performance, reliability, scalability, interoperability, and virtualization. The idea of cloud computing is covered in the paper, along with a number of issues and challenges that need to be resolved for the cloud to really be deployed and become a major aspect of our life in order for us to thrive.

Numerous solutions are being addressed by cloud computing in a private view. Despite this, cloud features are currently generally understood, particularly when looking at businesses. However, there are several security flaws in this feature that remain a difficult problem in a cloud context. As more companies utilise cloud technology, cloud computing is growing daily, yet various security concerns are also coming up. When moving its data to remote locations, every organisation choose a secure infrastructure. The main barriers to cloud computing adoption, according to NIST security, are portability and interoperability. Because cloud computing allows organisations to develop apps and services more quickly and outsource the responsibility of maintaining their infrastructure to the cloud service provider, it gives them more freedom. This delegation of authority allows the organisation to focus on projects with a business focus instead of infrastructure management.

References

[1] Akbar, H., Zubair, M., & Malik, M. S. (2023). The Security Issues and challenges in Cloud Computing. *International Journal for Electronic Crime Investigation*, 7(1), 13-32.

[2] AlSelami, F. A. (2023). Major Cloud Computing Security Challenges with Innovative Approaches. *Tehnički glasnik*, 17(1), 141-145.

[3] Arora, R., Parashar, A., & Transforming, C. C. I. (2013). Secure user data in cloud computing using

encryption algorithms. *International journal of engineering research and applications*, 3(4), 1922-1926.

- [4] Chaudhari, A. R., Gohil, B. N., & Rao, U. P. (2023). A review on cloud security issues and solutions. *Journal of Computer Security*, 31(4), 365-391.
- [5] El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering*, 29(1), 223-246.
- [6] Gimba, U. A., Ariffrin, N. A. M., Musa, A., & Babangida, L. (2023). Comprehensive analysis of security issues in cloud-based Internet of Things: A survey. *Journal of Computer Science & Computational Mathematics*, 13(2).
- [7] Gou, Z., Yamaguchi, S., & Gupta, B. B. (2017). Analysis of various security issues and challenges in cloud computing environment: a survey. In *Identity Theft: Breakthroughs in Research and Practice* (pp. 221-247). IGI global.
- [8] Joshi, M., Budhani, S., Tewari, N., & Prakash, S. (2021, April). Analytical review of data security in cloud computing. In *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)* (pp. 362-366). IEEE.
- [9] Kunduru, A. R. (2023). Security Concerns and Solutions for Enterprise Cloud Computing Applications. *Asian Journal of Research in Computer Science*, 15(4), 24-33.
- [10] Lalitha, P., Yamaganti, R., & Rohita, D. (2023). Investigation into security challenges and approaches in cloud computing. *Journal of Engineering Sciences*, 14(08).
- [11] Masadeh, S. R., AlShrouf, F. M., & Kumar, A. S. (2023). Concerns from Cloud Security Issues: Challenges and Open Problems. *International Journal*, 12(1).
- [12] Mondal, A., Paul, S., Goswami, R. T., & Nath, S. (2020, January). Cloud computing security issues & challenges: A Review. In *2020 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-5). IEEE.
- [13] Murigi, G., & Mutuku, M. (2022). Security issues and challenges in cloud computing among public institutions in Africa. *J. Bus. Manag. Sci*, 10(3), 131-137.
- [14] Nadeem, M. A. (2016). Cloud computing: security issues and challenges. *Journal of Wireless Communications*, 1(1), 10-15.
- [15] Osmani, N. M., Fatima, S., Ansari, A., & Bari, M. A. (2023). Cloud Computing Security Challenges, Threats and Vulnerabilities. *Mathematical*

- Statistician and Engineering Applications*, 72(1), 1446-1454.
- [16] Pandey, N. K., Kumar, K., Saini, G., & Mishra, A. K. (2023). Security issues and challenges in cloud of things-based applications for industrial automation. *Annals of Operations Research*, 1-20.
- [17] Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, 114, 102580.
- [18] Radwan, T., Azer, M. A., & Abdelbaki, N. (2017). Cloud computing security: challenges and future trends. *International Journal of Computer Applications in Technology*, 55(2), 158-172.
- [19] Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. *Procedia Computer Science*, 110, 465-472.
- [20] Rani, R. (2023). Security Issues and Challenges in Cloud Computing. *Multidisciplinary Approach in Arts, Science & Commerce (Volume-3)*, 82.
- [21] Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, 48, 204-209.
- [22] Razi, M., & Batan, A. (2023). Opportunities and Challenges of Cloud Computing in Developing Countries. *Artificial Intelligence in Society*, 3(1), 1-8.
- [23] Sasubilli, M. K., & Venkateswarlu, R. (2021, January). Cloud computing security challenges, threats and vulnerabilities. In *2021 6th international conference on inventive computation technologies (ICICT)* (pp. 476-480). IEEE.
- [24] Sethi, S., & Sruti, S. (2017). Cloud security issues and challenges. In *Resource Management and Efficiency in Cloud Computing Environments* (pp. 89-104). IGI Global.
- [25] Sharma, A., & Singh, U. K. (2021, September). Investigation of Cloud Computing Security Issues & Challenges. In *3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIC 2021)* (pp. 445-453). Atlantis Press.
- [26] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, 88-115.
- [27] Singh, K. P., Rishiwal, V., & Kumar, P. (2018, February). Classification of data to enhance data security in cloud computing. In *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)* (pp. 1-5). IEEE.
- [28] Singh, S. K., & Singh, D. K. (2017). Cloud computing: Security issues and challenges. *International Journal of Advances in Engineering & Technology*, 10(3), 338.
- [29] Sinha, A., Singh, N. K., Srivastava, A., Sen, S., & Sinha, S. (2023). Cloud Computing Security, Risk, and Challenges: A Detailed Analysis of Preventive Measures and Applications. *Machine Intelligence, Big Data Analytics, and IoT in Image Processing: Practical Applications*, 225-267.
- [30] Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, 76(12), 9493-9532.