IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

EXPLORATION ON DATA SECURITY ISSUES AND SOLUTIONS IN CLOUD COMPUTING

Yerrola Srinivas Tarun Sai Goud, Bachelors of Computer Science Engineering
Computer Science Engineering, Malla Reddy Institute of Technology, Hyderabad,
Allam Giridhar Nikhil, Bachelors of Computer Science Engineering, Computer Science Engineering, Malla Reddy Institute of Technology, Hyderabad.
Vundecode Adithya Krishna, Bachelors of Computer Science Engineering, Computer Science Engineering, Malla Reddy Institute of Technology, Hyderabad.

ABSTRACT

The term "cloud computing" refers to a form of technology that, rather than storing data on servers or local drives, offers distant services over the internet for the purpose of managing, accessing, and storing data. Serverless technology is another name for this particular technology. One of the most rapidly developing technologies in the field of computing is cloud computing. Many advantages and minimal security problems characterise cloud computing. This paper's goal is to examine, and then propose answers to, the many data security issues that crop up while using cloud computing in a multi-tenant setting. Additionally, models of cloud computing, including deployment models and service delivery models, are discussed in this work. When it comes to any kind of business or cloud computing, data is of the utmost importance. Companies can go under if their data is corrupted or lost, which can damage public trust and lead to financial ruin. At the moment, cloud computing is utilized either directly or indirectly by a great number of enterprises. In the event that a data breach occurs in cloud computing, it will have an impact not only on cloud computing but also on the commercial operations of the firm. It is for this reason that cloud computing firms are paying a greater amount of attention to the security of their customers' data.

Keywords: Cloud computing, data security, Cloud Services.

1. INTRODUCTION

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort and or service provider interaction," says the National Institute of Standards and Technology (NIST). "A model for enabling on-demand network access to a shared pool of reconfigurable computing resources"[1] is what cloud computing is. One of the most ubiquitous paradigms in the data processing industry is cloud computing, which involves providing computing infrastructure and solutions as a service.

Cloud computing is something that the majority of us use without even realising it, such as Gmail, Office 365, Dropbox, and other similar services. Global public cloud revenue is projected to increase from $80 billion in 2015 to $167 billion in 2020, according to a recent Forbes poll [2].

The use of cloud computing offers a multitude of advantages, including reduced financial outlay and accelerated access to infrastructure, accessibility at any time and from any location, and improved geographic coverage in a shorter amount of time. In addition, cloud computing eliminates the need for customers to worry about software licences, upgrades, and maintenance, hence reducing the amount of user participation [3]. Given the many advantages of cloud computing, many small and medium-sized organisations have already made the switch or are planning to do so soon.

The process of migration gives businesses the freedom to concentrate on their core business processes, which in turn allows them to grow their profitability, rather than concentrating on the IT infrastructure. There are also a number of important problems associated with cloud computing, which makes it challenging for a number of businesses and government organisations to transition to cloud computing. Most problems with cloud computing stem from inexperience and a lack of knowledge on how to properly secure and protect data stored in the cloud. This study mainly focuses on cloud security. It turns out that cloud security is more vulnerable because of the architectural core characteristics of cloud computing, including heterogeneity, resource sharing, multi-tenancy, virtualization, mobile cloud computing, and Service Level Agreement (SLA). A rise in security concerns stemming from the accumulation of digital assets is being voiced by an increasing number of concerned parties, as cloud computing becomes more popular among enterprises [4]. Cloud computing's operational environments (multi-tenant, heterogeneity, virtualization, etc.) are substantially different from conventional computing's, rendering typical security solutions ineffective in the cloud.

When it comes to traditional computing, there is a significant divide between those who are within the system and those who are not, and the security administrator is the lone person responsible for ensuring that the security standards are followed and that the data and assets are protected. The distinction between those who are insiders and those who are outsiders in cloud computing is quite hazy, and there are instances in which those who are outsiders become insiders. Due to the fact that cloud computing supports several tenants, it is extremely vulnerable to malevolent inside attackers as well as side attacks from outsiders. In light of this, cloud computing need to be equipped with a multi-tiered security method that is supported by service delivery models and deployment models.

There has been a deluge of research on cloud computing security, and it has covered a lot of ground. In [4, 5], we find a survey of security concerns related to service delivery mechanisms.
The former [4] focuses particularly on the Software as a Service (SaaS) paradigm, while the latter presents a more general overview of the subject. The authors of [6, 7] conducted a survey of the security vulnerabilities that are present in the deployment models, and they also suggested ways for mitigating such issues. The authors of [4, 6, 8] conducted a survey on the data security and privacy concerns that are associated with cloud computing. There was a survey conducted by other authors [9, 10] on the subject of security concerns pertaining to networks and infrastructure. The authors of [7, 8, 11] bring attention to the security concerns that are associated with multitenancy and virtualization. By utilising the services that are offered by cloud computing providers, this article takes a novel approach to bringing to light the security concerns that are associated with cloud computing. It also provides ways to minimise or lessen the impact of security threats.

The use of cloud computing comes with a number of benefits, including accessibility at any time and from any location, improved geographic coverage in the shortest amount of time, and reduced investments in infrastructure, among other advantages. However, cloud computing also presents a number of obstacles, including concerns over data security, a lack of resources and experience, and other similar issues. Data security is a major issue, and this study aims to address that issue by exploring the challenges of data security in cloud computing and offering possible solutions.

With the purpose of presenting the cloud computing model, this article has been organised. Additionally, it presents a variety of issues in the realm of data security and offers ways to addresses those challenges. In addition, this article finishes with a discussion of recent advancements and challenges in cloud computing.

2. LITERATURE REVIEW

2.1. Common Threats to Cloud Computing Security

There are a lot of typical threats to cloud computing. The reason behind this is that the platform relies only on technology, leaving it open to cyber assaults at any time. For instance, data breaches occur often in this context. The consequence is either data theft or illegal access. In addition, data breaches disclose the private information of an organisation, which leads to negative consequences for both the organization's reputation and its finances. In this regard, a previous investigation [12] was carried out. According to the findings of the researchers, data breaches compel businesses to install stringent security measures in order to safeguard their data. In addition, attacks using malware are extremely common in this area. One such assault involves the use of malicious software that can breach the cloud server and steal all of the necessary data. Another study [13] investigated the use of machine learning to provide predictions about attacks of this kind. This is an excellent method that technology companies can implement in order to protect their data.

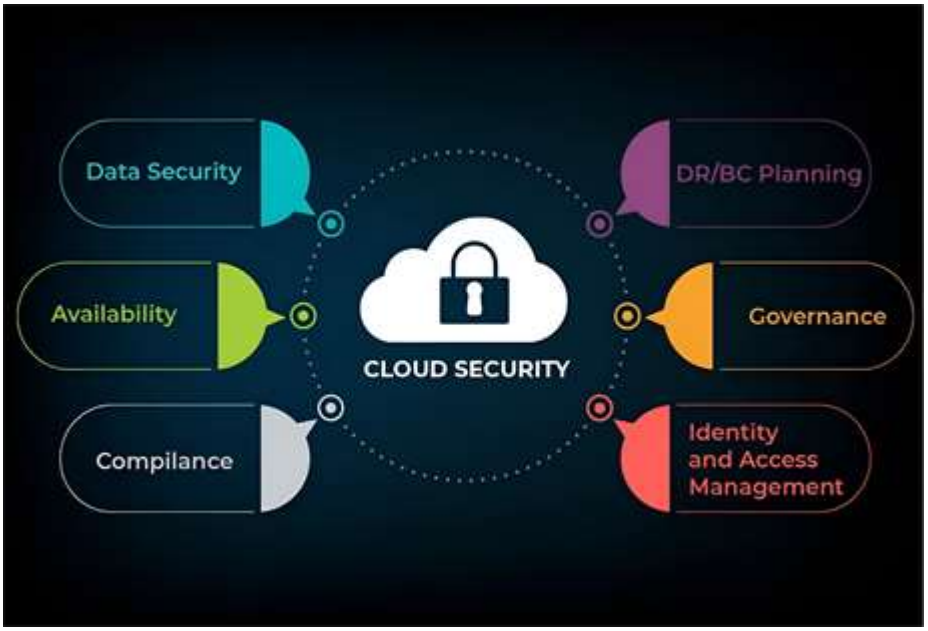

Figure 1. Data security and cloud computing.

Also becoming commonplace in the cloud computing industry is the practice of account hijacking. Its primary use case is in the context of identity theft schemes.

In this scenario, the attacker makes advantage of the private information of a person in order to carry out any other activity that is either unauthorised or questionable. Impersonating a person is typically accomplished through the use of hijacked email accounts. A previous study [14] that looked into this matter offered various preventative measures. Data and confidential information must be encrypted due to the circumstances. Distributed denial of service (DDoS) assaults are particularly common in the cloud. If these assaults are successful, they will cause a company's system to experience abnormally high levels of traffic, as stated in [15]. The company's image could take a serious hit because of them.

2.2. Mitigation Strategies in Cloud Security

Various preventative measures are implemented in order to guarantee the safety of cloud access. However, the approaches that are used for encryption are the most prevalent. Encryption is a method for protecting sensitive information by transforming it into a form that cannot be read without special decryption keys. Data storage safety has been prioritised, leading to the implementation of specific encryption algorithms [16]. These approaches proved to be quite effective in ensuring the security of cloud computing.

Within the context of a cloud network, the advantages of encryption are illustrated in Figure 2. Equation (1) is a mathematical mathematical expression that can be used to illustrate how effective encryption is in maintaining the integrity of data.

$$\text{DataIntegrity} = \frac{\text{NumberofCorrectlyDecryptedMessages}}{\text{TotalNumberofEncryptedMessages}} \times 100\% \quad (1)$$

Another method that is commonly used in this scenario is IAM. As stated in [17], the least privilege concept is used by Identity and Access Management (IAM) to control who can access what in a cloud context. Private information can only be accessed by authorised users.

Figure 2. Security in a cloud environment.

2.3 Emerging Trends in Cloud Security

Within the realm of cloud security, numerous new trends are currently emerging. Containerisation is a good illustration of this concept. The development and implementation of software applications and their dependencies are included in this method. Contained in portable containers, these apps and their dependencies provide isolation and allow for rapid development.

Based on the findings of [18], this strategy successfully ensures the security of cloud storage. There is a possibility that organisations would confront difficulties in terms of data governance and regulatory compliance while using this technology. Therefore, it is essential to make certain that the sensitive data contained within containers, such as HIPAA or DGPR, comply with the standards that govern the industry. Another concept that is becoming increasingly popular and is quite effective is serverless computing. Using this method, developers can build and run application scripts independently of servers and backend infrastructure by first creating an application model [19].

Amazon Web Services Lambda, IBM Cloud, and Google Cloud are a few illustrative instances. Serverless computing has many advantages, but it also raises integration difficulties, particularly when it is used with pre-existing on-premises systems or with services provided by third parties. In order to effectively maintain both security and performance, it is essential to guarantee that serverless services and other components of the application architecture are able to communicate with one another in a seamless manner.

In addition, machine learning and artificial intelligence are rapidly being utilised to guarantee the safety of cloud storage. Detecting and mitigating cloud threats is made easier with the help of these techniques, which utilise automated systems. There has been research conducted to investigate how effective these methods are in cloud computing. These approaches were discovered to significantly improve the performance of cloud servers while also ensuring a high level of security with their implementation. Additionally, they contribute to the improvement of threat detection and mitigation; yet, the implementation of these systems presents issues with regard to the openness of models and the privacy of data. This means businesses need to look at data protection laws and other regulations, as well as the ethical considerations around the use of AI algorithms to safeguard data.

Quantum computing, often known as QC, is another method that is now being utilised. Those who use the cloud have the ability to access a variety of quantum resources online and execute quantum algorithms without the need for specialised gear. According to [20], quality control has the potential to revolutionise technology companies in the future. Although the goal of quantum computing is to tackle difficult computational problems, the incorporation of quantum computing into cloud infrastructures raises worries about the potential for cryptographic flaws. To solve this problem and protect sensitive data kept in the cloud, businesses must find encryption methods that are resistant to quantum computing.

3. THE NEED FOR CLOUD SECURITY: CLOUD SECURITY CHALLENGES

3.1 Cloud Misconfigurations

An attacker can gain unauthorised access to vital resources by lateral movement across a network or a system that is not setup properly. This kind of attack carries a high risk of serious harm. Several factors can lead to misconfigurations, such as insufficient security awareness while setting up cloud services, human error, or incorrectly stated automated templates.

3.2 Data Privacy and Confidentiality

Many businesses prioritise the security of personal information and data confidentiality. Organisations must ensure the security of customer data in line with data protection regulations, such as the EU's General Data Protection Regulation (GDPR), the US's Health Insurance Interoperability and Accessibility Act (HIPAA), and the PCI DSS. Moreover, most businesses have private or sensitive information that isn't encrypted yet might cause serious damage to the business if leaked. The transfer of data to the cloud offers a multitude of advantages, but it also raises significant concerns regarding data security. When cloud-based storage systems are not properly secured, they are frequently exposed to public networks by default. This can make data easily available to malicious actors. The competence necessary to ensure that the cloud is configured and deployed in a secure manner is lacking in many organisations who are in the process of transferring their data and workloads to the cloud. The danger that sensitive data that has been moved to the cloud will be compromised occurs as a result of this, which can result in costly audits, compliance fines, and damage to the reputation of the organisation.

3.3 Social Engineering and Credential Theft

Threat actors often use cloud-hosted applications and environments in their social engineering campaigns. The prevalence of cloud-based email and file sharing platforms like G-Suite, Google Drive, Office 365, and OneDrive makes it easier for cybercriminals to trick workers into giving them access to sensitive data. All that's needed is to send the user a link, ask for access to the data, and give a good enough justification for them to let it through. There is a plethora of options available to cybercriminals who want to compromise employee credentials to cloud services. Organisations confront a major obstacle when trying to secure their

identities in the cloud. This is because critical data and services stored in the cloud are at risk when identities are hacked.

3.4 Specific Compliance Requirements

Organisations must show they have adequately limited access to sensitive information (such credit card details or medical records) in order to prove they are in compliance with most data protection laws. To make sure that only authorised workers can access the protected data, it may be necessary to create a physical or logical isolation within an organization's network. In addition to having a very different organisational structure compared to typical data centres, cloud deployments offer a restricted level of visibility and control over the infrastructure. It may become more challenging to accomplish and demonstrate compliance with these kinds of regulations when using cloud computing as a result of this.

4. TYPES OF CLOUD SECURITY SOLUTIONS

In order to ensure the safety of your cloud, you can make use of the following popular sorts of solutions.

4.1 Cloud Access Security Broker (CASB)

As a means of enforcing security policies, cloud service providers and suppliers have set up the Cloud Access Security Board (CASB). Its responsibility is to monitor user behaviour in relation to cloud-hosted resources and make sure that the company's security policies are followed. Many different types of security policies are within CASB's purview:

- Authentication and authorization
- Single sign-on
- Credential mapping
- Device analysis
- Encryption
- Tokenization
- Logging and alerting
- Malware detection and prevention

4.2 Cloud Workload Protection Platform (CWPP)

The principal objective of the workload-centric security product CWPP is to safeguard workloads, which can be applications or other resources, that are running on one or more virtual machines (VMs), containers, or serverless activities. One unique aspect of CWPP is that it safeguards workloads as a single entity, regardless of how they are dispersed across multiple servers or cloud instances in different data centres or clouds.

Typical capabilities of CWPP include the following:

- System hardening and system integrity monitoring
- Vulnerability management

- Host-based segmentation
- Application control
- Visibility of workload security across hybrid environments
- Central control of workload security from a single console

4.3 Cloud Security Posture Management (CSPM)

Continuous security posture monitoring (CSPM) solutions keep cloud security risks under constant watch. Along with finding, recording, and reporting security concerns, they can sometimes automatically fix them as well. Cloud service misconfiguration, mismatched security settings, resource control issues, and regulatory compliance violations are all instances of this kind of problem.

CSPM solutions prioritise the following four primary areas:

1. Asset inventory and classification
2. Identity, security and compliance
3. Monitoring and analysis
4. Cost management and resource organization

4.4 Cloud Infrastructure Entitlement Management (CIEM)

The cloud-based centralised system known as Identity and Access Management (IAM) is an expansion of CIEM. Even while IAM is the backbone of public cloud identity and access management, administering it with tools offered by first-party cloud providers gets too hard very fast. Concerns about complexity can be addressed by CIEM systems, which offer centralised identity and access governance rules. Reducing the amount of privileges needed for critical cloud infrastructure and making least privilege access control easier to implement in dynamic distributed systems are the primary objectives.

4.5 Cloud-Native Application Protection Platform (CNAPP)

CSPM and CWPP solutions are brought together on a single platform to establish the new category known as CNAPP. With the help of a CNAPP solution, businesses can fix security holes and incorrect settings, analyse security incidents in production settings, and react quickly to any threats they find. Hosts and workloads, such as containers, serverless operations, and virtual machines (VMs), are protected by this solution.

5. CLOUD SECURITY BEST PRACTICES

5.1 Understand the Shared Responsibility Model

The security duties of cloud providers are split between the vendor and the customer, according to a model known as shared responsibility, which facilitates cloud vendor operations. Protecting the underlying infrastructure is often the responsibility of the cloud provider; however, users are typically responsible for ensuring the security of their own workloads and data stored in the cloud. distinct delivery models have distinct responsibilities; for instance, IaaS, SaaS, and PaaS all stand for infrastructure as a service, software as a service, and platform as a service, respectively.

In general, the ability to exert a larger degree of control over the infrastructure results in an increased level of responsibility for the protection of the environment.

5.2 Perform Regular Audits and Penetration Testing

Identifying and addressing security flaws is the goal of penetration testing, which is a simulated attack that is authorised and carried out by ethical hackers. Potentially, it will help you assess your cloud infrastructure's security policies and fix any problems or vulnerabilities discovered. In order to ensure compliance and security, regulatory agencies often demand periodical audits, which are also highly recommended as security practices. Cloud security measures, whether implemented by you or your provider, can be more easily confirmed with its help.

5.3 Secure User Endpoints

The most popular way for endpoints in cloud environments to connect to the environment is through web browsers, however there are other options as well.

The implementation of client-side security, which ensures that end-user browsers are kept up to date and secure, grants organisations the ability to safeguard their workloads and data. Many security solutions can be used to protect your network from endpoint threats. These include firewalls, antivirus software, intrusion detection tools, mobile device security, Internet security tools, and endpoint security solutions.

5.4 Set Up Backup and Recovery Solutions

Features like high availability and durability are offered by cloud service providers in accordance with the shared responsibility paradigm. Unfortunately, data loss can still occur despite the capabilities mentioned before. Data loss can occur for a variety of reasons, including ransomware infections, accidental or malicious data deletion or modification, and hardware failures. To mitigate this risk, it is recommended to use backup and recovery systems.

Organisations have the ability to apply a variety of solutions for archiving, backup, and recovery of their data. Keeping recoverable copies can be made easier with the use of automated backups and lifecycle policies. Through the usage of archives, you are able to store data that is only used occasionally in a separate and safe location. In the event of a disaster or security breach, recovery procedures spell out the steps to restore data and identify who is responsible for overseeing the process.

5.5 Cloud Security with HackerOne

In the process of moving code, applications, and assets to the cloud environment, additional dangers are introduced. Through the utilisation of a robust community of ethical hackers who bring a unique skill to the table in order to discover vulnerabilities that scanners and AI miss, the unified platform that HackerOne offers handles the cloud security issues. Organisations are able to secure their cloud environment against many threat vectors by utilising the built-in visibility and reporting capabilities that HackerOne offers. Cloud misconfigurations, data exposures, subdomain takeovers, unauthorised application access, and many more exist as security vectors. Businesses who are trying to reduce their vulnerability to attacks in the cloud can benefit from three of HackerOne's main products:

1. HackerOne Assessments offers a fresh perspective on cloud pentesting, driven by the community. This technique expands coverage, provides real-time results, and streamlines remediation workflows, allowing organisations to quickly uncover and address vulnerabilities. By collaborating with background-checked, AWS-certified hackers, HackerOne offers AWS-specific solutions that help organisations see cloud-specific dangers in areas such as APIs, serverless deployments, IAM risks, DNS management, and S3. You can easily transfer vulnerability data and intelligence from HackerOne to AWS Security Hub so you can take quick and effective security measures.

2. The HackerOne Bounty encourages ethical hackers to assist organisations in identifying and resolving cloud security vulnerabilities, therefore reducing the likelihood of intrusions.
3. By assisting organisations in implementing a vulnerability disclosure policy, HackerOne Response helps them comply with regulations and provides security teams with intelligence on vulnerabilities across various cloud-based assets.

6. CLOUD COMPUTING ARCHITECTURE

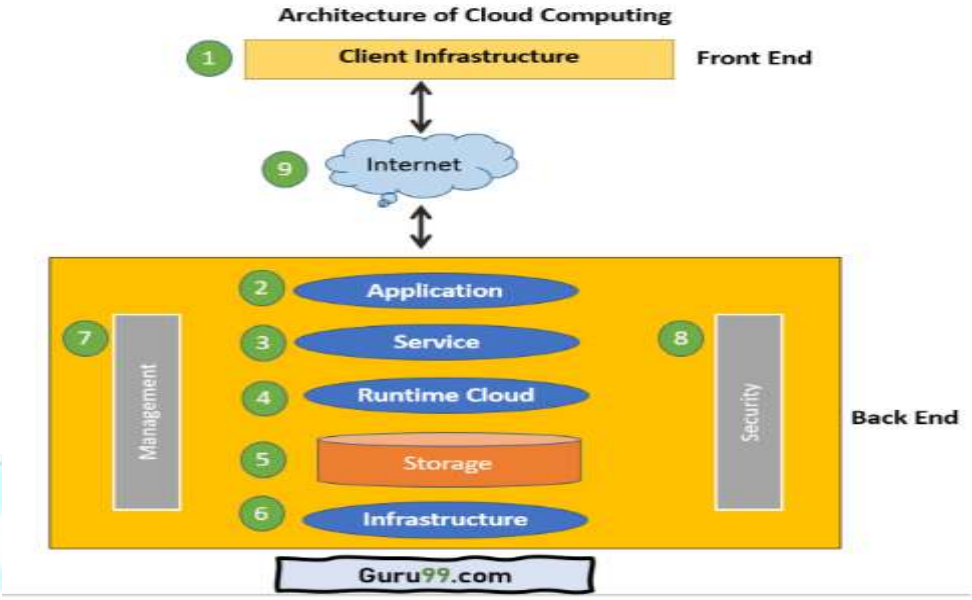

Figure 3: Architecture of Cloud Computing.

The architecture of cloud computing shown in figure 3 allows for scalability, which allows for the processing of enormous amounts of data within a tenant organisation. Certain qualities, including as resource pooling, self-service, measurement services, and wide network access, have the potential to enhance the architecture of a cloud environment. SOA (Service Oriented Architecture) and EDA (Enterprise Data Architecture) (Event Driven Architecture) are coupled in cloud computing architecture. In addition to client infrastructure and applications, the architecture of cloud computing includes runtime, storage, infrastructure, administration, and security. Cloud computing also includes management and security.

An architecture that is visible to the client or user is referred to as a frontend architecture. Included in this package are client-side APIs and apps that are essential for using cloud computing platforms. For the purpose of communication between the frontend and the backend, a network, such as the Internet, is utilised. In addition, the middleware makes it possible for the frontend to communicate queries to the backend. There are many different client sizes, as well as web servers, tablets, and smartphones, as examples.

6.1 Components of the Cloud Architecture

The Architecture of Components of the Cloud is shown in figure 4.

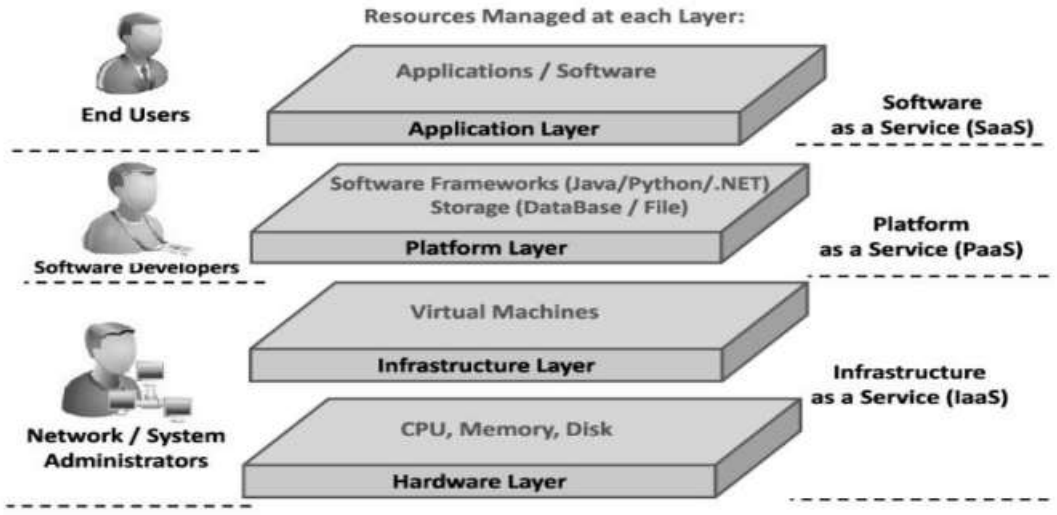

Figure 4: Components of the Cloud Architecture

Frontend of Cloud Computing Architecture: On the front end of the cloud computing architecture, each and every interaction that occurs within the user interface is displayed. The composition of a user interface is comprised of a number of subcomponents that collaborate with one another. There are four primary frontend components: the User Interface, the Client Infrastructure, the Software, and the Network.

Backend of Cloud Computing Architecture: The functionality of the frontend is made possible by the existence of the backend. It is made up of elements such as storage and hardware. One of the cloud service providers has complete authority over the backend of the cloud computing system. Regarding the backend of the cloud architecture, reliability is of the utmost importance because it is the component that keeps everything together. The primary components of the backend architecture are the application, the runtime cloud, the storage, the infrastructure, the management software, and the security.

CONCLUSION

This paper provides an overview of the major security concerns with cloud computing and the proposed solutions to these problems. But there are still some unanswered questions that may cause concern and even danger to certain die-hard CC supporters. In the end, we believe that cloud computing provides a great foundation for businesses to grow and thrive. But you must exercise extreme caution when bringing one into your home. Consider their compliance standards and the presence of a risk and weakness management plan when making a thoughtful selection regarding your supplier. While cloud computing has great promise for both academics and businesses, several challenging challenges remain, such as virtualization, security, performance, stability, scalability, and interoperability. The article discusses cloud computing and the many problems that must be fixed before the cloud can be implemented and become an integral part of our lives if we are to prosper. In order to find suitable security solutions to swiftly neutralise emerging risks, this literature review evaluation on cloud computing security is designed. Data privacy and security are major concerns when it comes to cloud computing. Security in the cloud is precariously balanced due to factors such as heterogeneity, resource sharing, virtualization, mobile cloud computing, SLAs, and multi-tenancy. Data security challenges and solutions are presented in this paper. Another new development in cloud computing is software-defined storage, which separates the logical storage services and capabilities from the underlying hardware. Another new concept is cloud-of-things, which combines cloud computing and the Internet of Things (IoT) for smart city applications. Container-as-a-service (CaaS) is another example of this. There are new problems with cloud computing that have arisen as a result of all these new advances.

Data and privacy should be safeguarded by regularly reviewing and updating security policies and procedures in response to technological changes.

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. InIdentity 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. In2021 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] Kelly, D., Glavin, F. and Barrett, E. (2020) Serverless Computing: Behind the Scenes of Major Platforms. IEEE 13th International Conference on Cloud Computing (CLOUD), Beijing, 19-23 October 2020, 304-312. https://doi.org/10.1109/CLOUD49709.2020.00050

[13] Rath, M., Satpathy, J. and Oreku, G.S. (2021) Artificial Intelligence and Machine Learning Applications in Cloud Computing and Internet of Things. In: Kaur, G., Tomar, P. and Tanque, M., Eds., Artificial Intelligence to Solve Pervasive Internet of Things Issues, Elsevier, Amsterdam, 103-123. https://doi.org/10.1016/B978-0-12-818576-6.00006-X

[14] Abidin, S., Swami, A., Ramirez-Asís, E., Alvarado-Tolentino, J., Maurya, R.K. and Hussain, N. (2022) Quantum Cryptography Technique: A Way to Improve Security Challenges in Mobile Cloud Computing (MCC). Materials Today: Proceedings, 51, 508-514. https://doi.org/10.1016/j.matpr.2021.05.593

[15] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. and Ayaz, M. (2021) A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. IEEE Access, 9, 57792-57807. https://doi.org/10.1109/ACCESS.2021.3073203 [16] Yau-Yeung, D., Yigitbasioglu, O. and Green, P. (2020) Cloud Accounting Risks and Mitigation Strategies: Evidence from Australia. Accounting Forum, 44, 421-446. https://doi.org/10.1080/01559982.2020.1783047

[17] Gupta, I., Gupta, R., Singh, A.K. and Buyya, R. (2020) MLPAM: A Machine Learning and Probabilistic Analysis Based Model for Preserving Security and Privacy in Cloud Environment. IEEE Systems Journal, 15, 4248-4259. https://doi.org/10.1109/JSYST.2020.3035666

[18] Chen, C., Zhang, L. and Tiong, R.L.K. (2020) A Novel Learning Cloud Bayesian Network for Risk Measurement. Applied Soft Computing, 87, Article ID: 105947. https://doi.org/10.1016/j.asoc.2019.105947

[19] Kumar, M.S. and Raja, M.I. (2020) A Queuing Theory Model for e-Health Cloud Applications. International Journal of Internet Technology and Secured Transactions, 10, 585-600. https://doi.org/10.1504/IJITST.2020.10029365

[20] Amini, M. and Bozorgasl, Z. (2023) A Game Theory Method to Cyber-Threat Information Sharing in Cloud Computing Technology. International Journal of Computer Science and Engineering Research, 11, 4-11.