International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

A Three-Party Cloud Authentication Framework for Enhanced Security and Integrity

Rajesh Gundla[1], Sunil Gupta[2], C. Srinivasa Kumar[3]

[1]Research Scholar, CSE, Shridhar University, Pilani, Rajasthan, India

[2]Associate Professor, Dept. Of Computer science and Engineering, Shridhar University, Pilani, Rajasthan, India

[3]Professor, Dept. Of Computer science and Engineering, Vignan's Institute of Management and Technology for Women, Hyderabad, Telangana, India

Article Info
Volume 8, Issue 3
Page Number : 581-593

Publication Issue :
May-June-2021

Article History
Accepted : 15 June 2021
Published: 25 June 2021

ABSTRACT

This paper provides a comprehensive overview of the security and privacy issues faced by organizations using cloud computing. It defines cloud computing and discusses the different types of services and deployment models. The paper presents suggested solutions that can help organizations address operational, technical, and legal issues related to cloud computing while meeting the needs of users. Cloud computing providers must protect the sensitive data of their customers to provide reliable services, and the paper proposes various solutions to address these concerns. However, the authors caution that these solutions are not a complete picture of how fast technological innovation can occur. The paper emphasizes the importance of encryption in protecting the confidentiality and integrity of data and highlights the use of SSL encryption methods to secure web services that use the HTTPS protocol.

Keywords : HTTPS Protocol, Cloud computing, IT Services, Service Level Agreement

I. INTRODUCTION

The rise of cloud computing has made it easier than ever to store and analyze data. Since the term was first used in 2006, the public has started to understand how it can help organizations improve their efficiency and reduce their expenses. One of the main advantages of cloud computing is that it eliminates the need for maintaining and monitoring hardware and software. The concept of cloud computing combines the various computing paradigms known as grid, distributed, and virtualized. It allows a computer system to be adaptable and can run on different types of hardware. Besides being easier to store and analyze data, cloud computing also provides various benefits such as Internet access, on-demand resources, and computing as a Service. Due to the increasing number of people aware of the security issues associated with cloud computing, it has become a viable business model for providing IT services. However, there are still many security flaws that prevent organizations from using it properly.

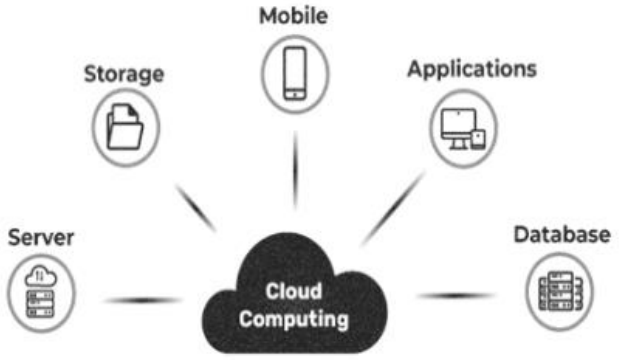

Figure 1: Cloud computing uses and its types

There are three different types of cloud computing services available: public cloud computing, private cloud computing, and hybrid cloud computing. Understanding the concept of cloud computing is very important to ensure that businesses can benefit from its various advantages. This study aims to provide a comprehensive overview of the technology. Besides being easier to store and analyze data, cloud computing also provides various benefits such as Internet access, on-demand resources, and computing as a Service. A service level agreement (SLA) is a type of agreement that governs the operations of cloud computing. It allows a group of computers to run as a single processing unit. The ability to develop and deploy real-time data analysis and applications has been made possible by cloud computing. The architecture of cloud computing is based on the Software-as-a-Service (SaaS) model, which brings together various technological components and the infrastructure needed to run applications. Another complicating factor when it comes to defining cloud computing is the number of viewpoints that have been used to define it. These definitions imply that the technology has several important characteristics. The infrastructure of cloud computing is generally cost-efficient and scalable. It can be easily accessed by businesses. It supports a wide range of applications and infrastructure, and it is flexible enough to change its features.

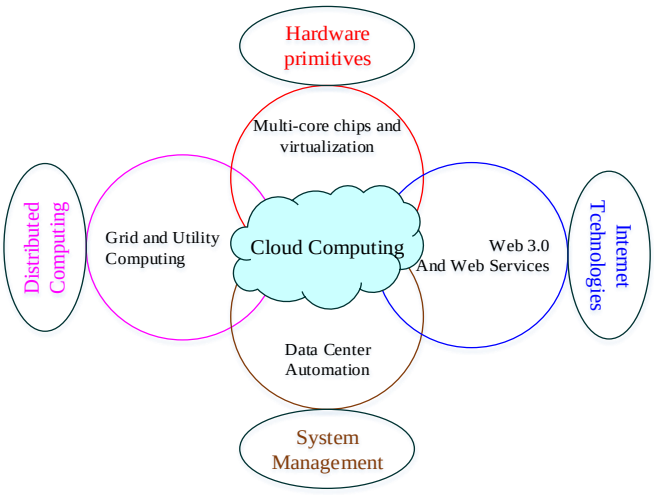

Figure 2: Evolution of the Cloud Computing Industry

The potential of cloud computing to benefit end users and IT developers is immense. It is quickly becoming one of the most critical factors in the evolution of the internet. Table 3.1 indicates that end users can choose from a wide range of cloud computing models to access these services.

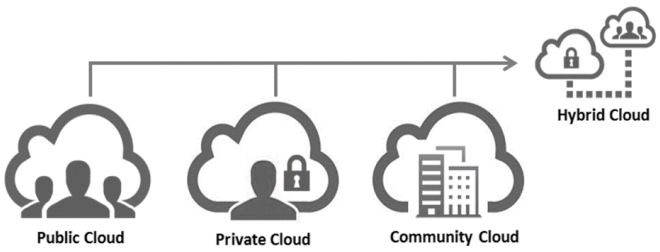

Figure 3: Types of cloud computing deployment models

Table 1 Deployments models for cloud computing

Architecture	Uses
Virtual Private cloud	Private cloud space is provided via the usage of a public cloud platform in this instance.
Public	The Saas platform's registered users may use the cloud services in this method.
Private	Workers in a company's I.T. department are only allowed access to cloud services under this model.

Hybrid	The less-sensitive data applications of the companies are hosted by the public cloud computing service provider (CSP).
Community	As a result, a significant number of organizations use the identical service models, but their access ids are never made public.

Business cloud	Cloud computing services may be accessed using this architecture.

2. Preliminaries:

Different cloud computing models are commonly used by end users. In the next section, we'll talk about the most popular models. The most popular cloud computing models include Infrastructure as a Service, Platform as a Service, and Software as a Service. One of the most popular cloud computing models is the Platform as a Service, which allows end users to create and manage their own applications. One of the most popular cloud computing models is the Infrastructure as a Service, which allows end users to store their data on a server. Google's approach is to create a single platform for all of its services, which makes it easier for customers to use. The cloud computing architecture shown in the picture is typically constructed on the basis of the layers shown in Figure 3.5. This type of design is referred to as a three-layered cloud structure.

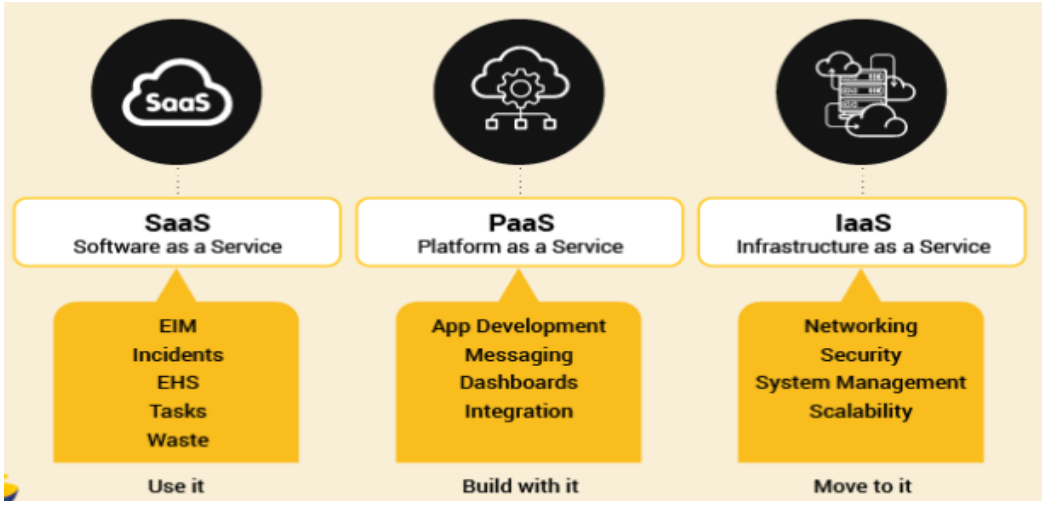

Figure 4 : Cloud service model types

Table 2 Cloud service Models

Service Model	Uses	Examples
Infrastructure as a service (Iaas)	These customers' data may be saved on this server since it is only utilized for this function.	KVM, ceph
Software as a service (Saas)	This channel allows you to connect to the provider's server-side software via the use of a web browser.	IBM lotus Live

Everything as a service (Xaas)	Assembling the many services onto a single platform in order to make it easier for customers	Google provides all the above services.
Platform as a service (Paas)	Using this service, users may create their own apps or programmers by using a runtime environment provided by the service.	Git-Hub, Kubernetes and Docker.

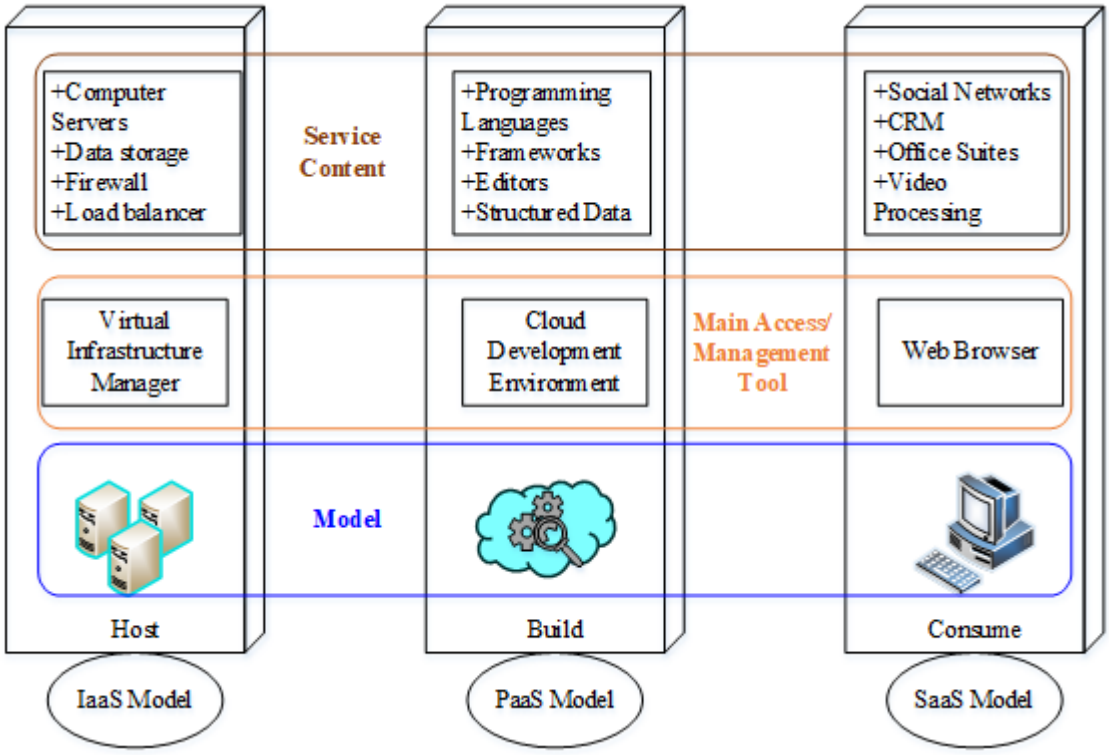

Figure 5 Three-layered Cloud Model

(1) IaaS Model

Various hardware components, such as storage and servers, are distributed through the cloud computing architecture. These components are used to deliver services that are available at any time. Amazon Web Services is an example of a cloud computing model that provides customizable infrastructure as a service.

(2) PaaS Model

One of the most important advantages of cloud computing is its ability to provide a wide range of flexible and customizable applications. Unlike traditional infrastructure, the cloud model focuses on abstraction. This allows developers to create programs without having to know anything about the specific hardware components that are used in their applications. One of the most popular platforms for developing applications is Google App Engine, which is a PaaS paradigm.

(3) SaaS Model

The Software as a Service model makes it easier for end users to access services by using online portals. This type of paradigm eliminates the need for them to develop and maintain their own applications. Oracle CRM utilizes a SaaS model to allow its end users to access the software. One can create a hybrid or private cloud environment

using the three main cloud models shown in Figure 1.3. The difference between public, hybrid, and private cloud infrastructures is shown in Figure 1.3. These are some of the most essential and widely used services in the cloud computing industry. Various types of cloud services, such as multi-cloud, distributed, and communal, are also available. Private clouds only allow a single user to access all of the resources, and they are more secure than public clouds. One of the most common reasons why organizations choose to use a private cloud is to protect their privacy while allowing them to profit from the shared resources. This type of architecture is ideal for applications that require direct control over their cloud.

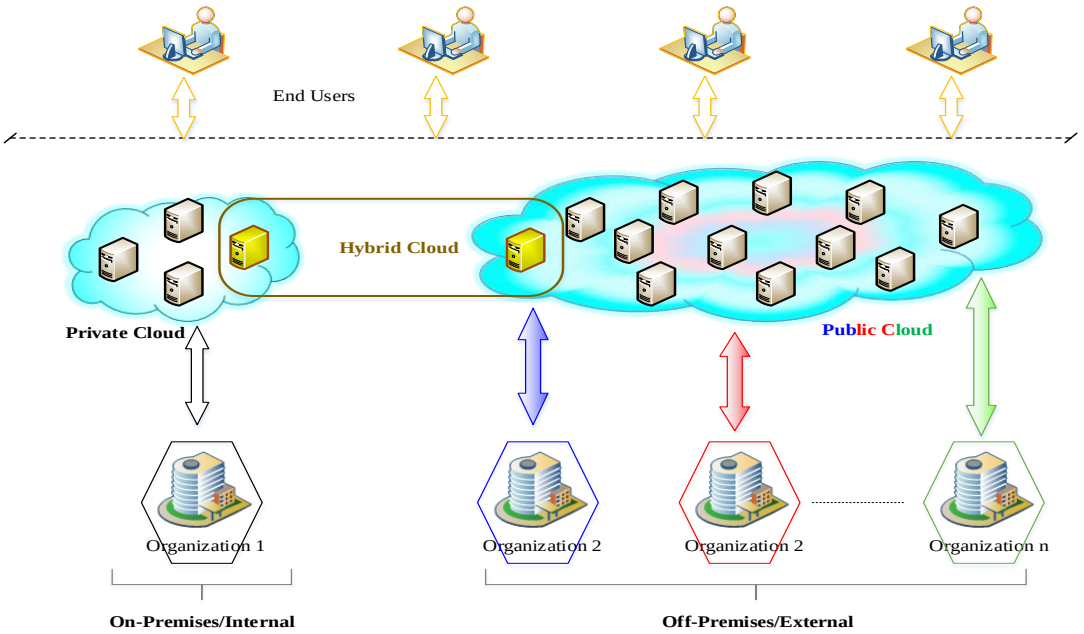

Figure 6 : Operational structure of cloud

Another common reason why organizations choose to use a public cloud is to lower their costs and provide the highest level of service. This type of architecture is simple to use and operates efficiently because it is a multi-organizational environment. Hybrid cloud computing solutions combine the advantages of both private and public clouds into a single integrated solution. This type of architecture allows organizations to have more flexibility and scalability by allowing workloads to be dispersed across multiple clouds.

II. Advantages and Applications

The advantages of cloud computing are numerous, such as allowing organizations to develop real-time applications. One of the most important advantages of cloud computing is its ability to provide customers with on-demand self-service. This type of solution allows them to monitor the various aspects of their server, such as its availability, performance, and network storage. One of the most important advantages of cloud computing is its ability to handle a large number of users. This type of solution can be very useful in situations where there is a need to handle a huge amount of data. In most cloud-based programs, users can access the cloud by connecting to the internet. One of the most important advantages of cloud computing is its ability to provide customers with better availability. This type of solution allows them to determine their own requirements at any moment. One of the most important advantages of cloud computing is its ability to provide customers with better service. This

type of solution can be very useful in situations where there is a need to handle a huge amount of data. With the help of artificial intelligence, the cloud will be able to make decisions based on the collected data.

A multi-tenant model is also known as computing resource pooling, which allows a cloud service provider to provide a variety of computer resources to its customers. This type of approach can be very useful for small and medium-sized businesses (SMBs) because it allows them to provide their customers with better services. One of the most beneficial features about cloud computing is its ability to offer users with easy maintenance and backup. This eliminates the need for them to perform manual repairs on their servers. The cost efficiency of cloud computing is one of the most important advantages it offers. Compared to traditional methods of data storage, it is more cost-effective to store and update data. One of the most important advantages cloud computing offers is its ability to provide users with unlimited storage capacity. This type of solution eliminates the need for them to limit their access to the data. It also allows them to access the stored data from anywhere. Another important advantage of cloud computing is its centralization, which allows it to store and manage data in a centralized manner. One of the most important advantages of cloud computing is its ability to provide users with better flexibility. This type of solution allows them to manage their various devices and applications easily. The various features of cloud computing make it an integral part of the development of real-time applications. For instance, Internet of Things (IoT) applications allow people to connect and communicate with billions of tiny devices. Due to the amount of data that these devices generate, the cloud allows users to analyze and store this data.

Table 3 : Cloud applications

Application	Description
E-Government	E-Government is the optimal replacement for traditional systems. The tradition system lacks in following perspectives, • Low scalability • Poor resource maintenance • Limitations in data availability With the cloud integration, the E-Government application can be implemented. This includes, • Payment and tax system • E-Police and E-court • Citizen Management System
E-Learning	It is operating upon collaborative involvement of teachers, researchers and students Introduction of E-learning has gained interests among the students Implementation of E-leaning with cloud computing includes, • Virtual classroom • Digital education norms • Virtual conferences and meetings • Multimedia teaching
	Traditional resource planning for enterprises has following issues, • Poor reliability • Unable to customize

Resource Planning	• Unaware of adaptions Thus, the cloud-based resource planning method has been developed The cloud application improves the overall system in terms of, • Supply chain and vendor system • Flexible finance and accounting • Production and delivery monitoring
IoT Applications	Cloud computing is the significant part of IoT applications. Some of the cloud based IoT applications are, • Smart city • E-healthcare • Intelligent transportation • Industrial IoT • Precision agriculture

A smart city is built using the cloud infrastructure, smart devices, and end users who can connect to the internet.

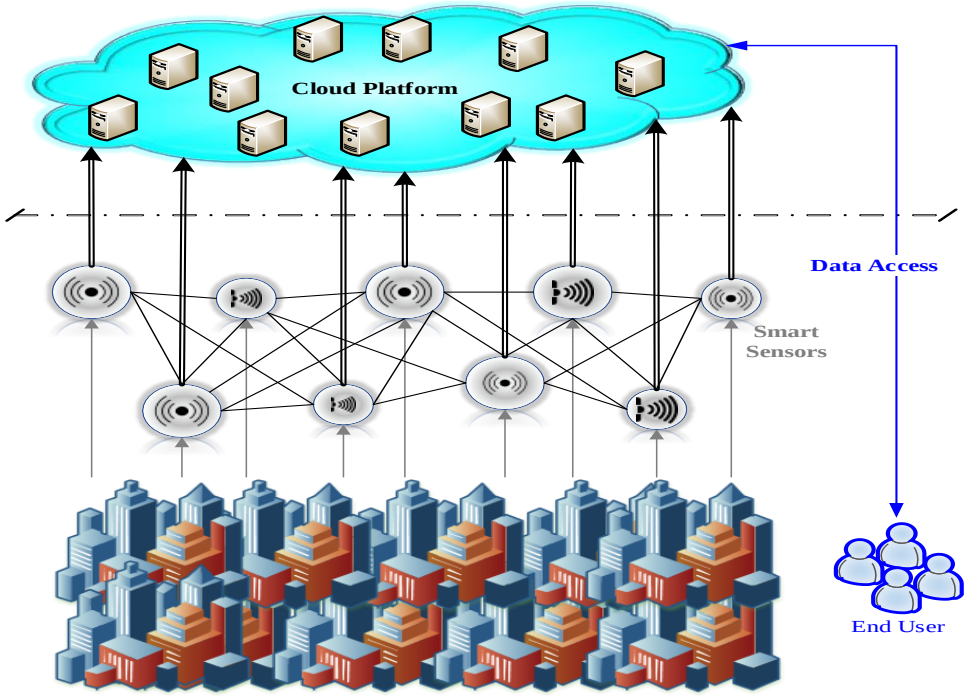

Figure 7 : Cloud-based smart city application

These devices are used for various tasks, such as monitoring the environment, traffic conditions, and structural monitoring. Due to the increasing complexity of the data collected by these devices, they can be more complex to manage. One of the most effective ways to reduce the overhead of these applications is by transferring the data analysis to the cloud. In an application scenario, the data collected by smart devices, such as sensors, actuators, and wearable devices, can be used to provide additional predictions. This type of solution can be made using the cloud to analyze and store the data. Without the help of cloud computing, IoT devices would not be able to handle the massive amount of data that these devices collect. Due to the increasing popularity of cloud computing, the development of smart applications has become more prominent.

III. Issues identified in cloud

Although there are many advantages to cloud computing, it also has many drawbacks that need to be resolved in order to benefit its users. One of these is its ability to handle the immense amount of data that it collects.

(1) Interoperability

One of the most important issues that cloud computing has is its lack of interoperability. This issue is caused by the varying requirements that different vendors have in order to work together. In order to achieve interoperability, the various cloud vendors need to implement specific protocols and data formats. The various levels of interoperability are designed to ensure that the services that are offered by the different cloud vendors are compatible with each other. This is done through the use of the same standards.

(2) Quality

Generally, the cloud services are provisioned based on the service level agreement (SLA). However, with the increasing number of users, the need for different services has increased. This means that the current approach to service provisioning is not able to meet the needs of the customers. In addition, the presence of security threats can affect the quality of service that cloud computing provides. This issue can prevent organizations from achieving optimal performance.

(3) Control

The lack of control and governance over the various aspects of the cloud computing environment can also affect the quality of the service that organizations provide. Most of the time, the management of the cloud services is carried out by the IT department. However, due to the nature of the cloud computing environment, the department's role in the provision and de-provisioning of services is no longer complete.

(4) Lack of expertise

Due to the increasing number of workloads that organizations are placing on the cloud, the lack of expertise in the management of these workloads can lead to various bottlenecks.

(5) Security

Due to the nature of the cloud computing environment, there are many potential vulnerabilities that can be exploited by third-party applications. These include the lack of control and governance over the various aspects of the cloud computing environment, the lack of visibility into the operations of the cloud, and the vulnerability of the data security. Some of the most common factors that organizations consider when it comes to the security of their cloud computing are the availability of resources and the physical security of their data center.

(6) Data Integrity

One of the most important factors that organizations consider when it comes to the security of their cloud computing environment is ensuring that the data they are storing is not tampered with. This is because hackers and attackers can easily access the content stored in the cloud.

(7) Heterogeneity

In real-world data, there is a huge amount of heterogeneity, which means that the cloud computing environment needs to be able to process and store all of it without experiencing any interruptions. Despite the various factors that have been considered, the cloud computing environment still has a long way to go before it can fully address these issues.

IV. Privacy, Security and Trust Challenges of Cloud Computing

When it comes to choosing cloud computing, security, privacy, and trustworthiness are some of the most crucial factors to take into account. Since they can now access processing power they would not be able to get with their own devices, individuals can now use cloud computing services to gain access to a virtual environment. In order to deliver this type of environment, data delivery via the cloud is also essential. This type of environment results in numerous security issues that need to be resolved in the future. In this tutorial, we'll talk about the basics of trust, privacy, and security in the context of cloud

computing. The concept of trust, privacy, and security is defined. This type of environment results in numerous security issues that need to be resolved. One of the most important factors that organizations consider when it comes to the security of their data is ensuring that it is obtainable, available, and reliable. Various concepts such as dependability, accountability, and authentication are used to describe the security of data. Always keep in mind that data should not be shared with anyone who is not authorized to access it.

The concept of privacy is a fundamental human right that individuals have to protect their private lives. This is why organizations consider various factors when it comes to protecting the privacy of their customers' data. They use laws, standards, and practices to ensure that their operations are conducted in a secure manner. Some of the most common privacy concepts that are used by businesses include transparency, consent, validity, data security, and accountability. The ability to accept one's weaknesses as long as one has faith in the good intentions of others is called trust. This concept is related to one's capacity to predict the future behavior of people and data. To establish trust, one must first have at least two individuals or machines working together. Meeting privacy or security objectives can help boost one's confidence. There are various factors that need to be considered when it comes to addressing the security, privacy, and safety concerns of data. The open architecture of cloud computing allows for various security and privacy issues to arise due to its processing and power distribution. When it comes to storing and managing one's data in the cloud, one must first ask if it is secure. Another important aspect to consider is if the companies that provide cloud computing services follow the law. There are various threats that can affect the operations of organizations using cloud computing. The CSA identified various risks that cloud computing could expose itself to. These include abuse of the system, data leaks, and unauthorized access. Other risks include the sharing of technology concerns, insider threats, and denial of service attacks. The National Institute of Standards and Technology (NIST) identified various security and privacy issues related to cloud computing as being linked to the technology that enables it. Three independent issues need to be addressed: Trust, Security, and Privacy.

Table 4. Challenges of cloud computing

Area/ Technology	**Security**	**Privacy**	**Trust**
Virtualization	Integrity	Personal data on a shared infrastructure should be segregated.	Some people may lose trust in the system when virtual machines and hypervisors have been altered.
Grid technology	Availability		Interoperability
Web services	Integrity and confidentiality	Confidentiality and security	Interoperability
Service-orientated architectures	Integrity		Distributed systems rely on a number of security credentials to function.
Web application	Integrity and availability		Trust in a variety of locations

frameworks			
Encryption in the cloud context	Confidentiality	Confidentiality and security	

5.1 Cloud computing security issues:

The sheer number of cloud computing services and their deployment methods expose them to various security risks. These are not the only concerns that cloud computing raises. One of the most important factors that users need to consider when it comes to cloud computing is their control over the resources that they use. If the data they have stored in the cloud is accessed by unauthorized individuals or entities, they will be held liable for any damages. Having the necessary level of control over the data in the cloud is very important to ensure that it is secure and accessible. One of the most effective ways to protect the confidentiality and privacy of data is by implementing encryption. Although end users can access the decryption keys, there are still many technological obstacles that need to be resolved in order to make it work.

In order to function properly, cloud computing requires the installation of access control systems. These systems should be able to prevent unauthorized access and use of the data stored in the cloud. Due to the evolution of the technology, the security of the applications and platforms that are used in cloud computing has become more critical. To ensure that they are secure, organizations should regularly update their security policies and procedures.

5.2 Cloud computing privacy issues:

Cloud computing allows organizations to store and access data and files critical to their operations. However, it can be very challenging for individuals and organizations to control the information that they commit to the cloud. Even though the cloud can store and process various types of data, it's important to consider the sensitive nature of the information that you store in it. Having this data in the cloud can help prevent it from being lost to competitors. One of the most important factors that users need to consider when it comes to cloud computing is their right to access the data that they have stored in the cloud. Since the storage capacity and processing power of the cloud are shared, users are more prone to experiencing data leakage. Keeping track of the data that you store in the cloud can be very challenging since it's often stored in different locations. Transferring data from one country to another requires the completion of agreements, and this can be impossible if the locations are unreliable. When it comes to externalizing privacy, users, as well as third parties, such as employees, should place their trust in the cloud computing company to uphold their promises.

5.3 Trust challenges of Cloud computing:

The establishment of trust is also a crucial aspect of the cloud computing process. Customers should place their faith in the service providers who offer cloud computing services. A cloud computing company must be able to address their customers' privacy and security concerns in order to gain their trust. This can help boost the market's confidence in the company. One of the most important factors that users and the cloud computing company need to consider when it comes to the establishment of trust is the dynamic addition of resources and users to the platform. This can be done through the use of various tools and techniques. Another important factor that users and the company need to consider is the security requirements of the cloud computing platform. Since the resources and users of the cloud are dispersed, they may have different requirements than those of local systems. The complexity of the cloud computing architecture and the lack of transparency in it can expose the platform to security vulnerabilities. These issues can also affect the processing capacity and data of the cloud users. Besides the security requirements, the company also

needs to ensure that it follows the best practices and laws when it comes to the management of its customers' data. This can help prevent unauthorized access and use of the platform. Building trust can be achieved by implementing assurance measures. One of the disadvantages of using cloud computing is that it can't guarantee that users will be able to keep their assets secure at all times.

V. Proposed Three-Party Cloud Authentication Framework

The following sections discuss the various security and privacy concerns that cloud computing users face.

A. When moving to the cloud, there are a number of things to keep in mind: Follow these guidelines and you can increase the security of your cloud computing environment. There are two types of security measures that are commonly used by cloud computing companies: partner-based and user-based. The former is the security measures that are carried out by the cloud service provider. One of the most important steps that a cloud computing company can take to improve its security is to develop a long-term strategy. Before you sign up for cloud computing services, make sure that you have a clear understanding of the company's security policy and procedures. We must also know who will monitor your data and have a plan for addressing security issues.

B. Monitoring system

The cloud provider should also regularly check the performance of the platform.

C. Measures must be done in the face of the top cloud computing dangers

6.1 Implementation:

Criminal activities are not allowed to use cloud computing for their purposes. It can also be used by insiders with bad motives and insecure interfaces. Security should be considered when it comes to implementing cloud computing solutions. The following table provides a list of implementation points for the different approaches.

Having a security strategy is also important to ensure that the company's operations are protected from the risks that come with cloud computing. Before signing up for a cloud computing service, make sure that it can protect your sensitive data. Before you commit to a cloud computing platform, it's important that you find one that has the necessary expertise to meet its service goals. Before you sign up for a cloud computing platform, make sure that it can provide a formal security policy. This should include a list of all the necessary rules and regulations that will be used to protect your data. Before signing up for any cloud computing platform, you should also know who will be monitoring your data. It should also be ready for a security breach. The measures that the cloud service provider will take following a security incident should be verified. Make sure that the access restrictions for your data are in place to prevent unauthorized access. This should be done to ensure that only authorized users can access your data.

6.2 Monitoring system

The cloud provider should also regularly monitor the performance of its platform.

6.3 Threats to Cloud Computing

It must be ready for a security incident. Care must be given during the validation and registration procedures. You should keep an eye on the public blacklists to see whether anyone has blocked your network. Insecure API and Interfaces Have to Be Assessed The security model of cloud providers' interfaces has to be thoroughly studied. The implementation of access restrictions and authentication methods should be carried out in a secure manner. Also, the human resources requirements of the company should be included in the legal contracts. Before you commit to a cloud computing service, make sure that it can protect your sensitive data. Conduct a comprehensive supplier evaluation and thoroughly manage your supply chain to prevent potential security breaches. It is necessary

to implement service level agreements. You should also regularly perform scans and configuration audits to identify potential vulnerabilities. Having strict access control and authentication methods is required for administrative access. The creation, destruction, and storage of key and other important components must be carried out in a robust manner. An effective monitoring system can also detect unauthorized behavior. Account information should not be shared by users and services.

VI. Experimental Results

A cloud computing solution should meet these six security standards. In simpler terms, it should be able to celebrate after a victory if it adheres to these security guidelines. Before you commit to a cloud computing service, make sure that it can protect your sensitive data. Having a security assessment is also important to ensure that the platform is secure.

Table 5: Security Requirements

Security Requirements	Cloud Deployment models								
	Public Cloud			Private cloud			Hybrid Cloud		
Identification & Authentication	√	*	√	√	*	√	*	*	√
Authorization	√	√	√	*	*	√	*	*	√
Confidentiality	*	*	√	*	√	√	*	*	√
Integrity	√	*	√	*	√	√	√	√	√
Non-repudiation	*	*	√	*	*	√	*	*	*
Availability	√	√	*	√	√	√	*	*	*
	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS
	Cloud Service Models								

A cloud computing deployment model or service model uses an arrangement of checkmarks and arrows to denote whether or not certain features are required. Various authentication methods such as smartcards, biometrics, and passwords are used to secure a cloud computing account. An access control policy also ensures that only authorized individuals can access the cloud at certain times.

VII. Conclusion

Cloud computing providers have to protect the sensitive data of their users and customers in order to maintain and provide reliable services. Due to the complexity of the issue, the team has created various solutions that can address these concerns. Unfortunately, the public should not rely on these solutions as a complete picture of how fast technological innovation can happen. An encryption method is necessary for any type of data. It can be used to check the integrity of the data by ensuring that all transactions are performed properly. This type of security measure is very important when it comes to protecting the confidentiality and integrity of data. In the case of web services that use the HTTPS protocol, an SSL encryption method is used to protect the information.

VIII. REFERENCES

[1]. Anbuchelian, S.; Sowmya, C.M.; Ramesh, C. Efficient and secure auditing scheme for privacy preserving data storage in cloud. Clust. Comput. 2019, 22, 9767–9775.

[2]. Babu, S. Dilli, and Rajendra Pamula. "An effective block-chain based authentication technique for cloud based IoT." Advances in Computing and Data Sciences: 4th International Conference, ICACDS 2020, Valletta, Malta, April 24–25, 2020, Revised Selected Papers 4. Springer Singapore, 2020.

[3]. Wang, H.; Wang, Z.; Domingo-Ferrer, J.: Anonymous and secure aggregation scheme in fog-based public cloud computing. Future Gener. Comput. Syst. 78, 712–719 (2018)

[4]. Wazid,M.; Das, A.K.; Kumar, N.; Vasilakos, A.V.: Design of secure key management and user authentication scheme for fog computing services. Future Gener. Comput. Syst. 91, 475–492 (2019)

[5]. Chandrakar, P.; Om, H.: A secure and privacy preserving remote user authentication protocol for internet of things environment. In: International conference on computational intelligence, communications, and business analytics, pp. 537–551, Springer, Berlin (2017)

[6]. Armando, A.; Basin, D.; Boichut, Y.; Chevalier, Y.; Compagna, L.; Cuéllar, J.; Drielsma, P. H.; Héam, P.-C.; Kouchnarenko, O.; Mantovani, J. et

al.: The avispa tool for the automated validation of internet security protocols and applications. In: International conference on computer aided verification, pp. 281–285, Springer, Berlin (2005)

[7]. Kumar, A.; Om, H.: Lightweight, ecc based rfid authentication scheme for wlan. Int. J. Bus. Data Commun. Netw. (IJBDCN) 12(2), 89–103 (2016)

[8]. Stallings, W.: Cryptogr. Netw. Secur. Pearson Education, India (2006)

[9]. Paar, C.; Pelzl, J.: Understanding cryptography: a textbook for students and practitioners. Springer Science and Business Media, Berlin (2009)

[10]. Ray, S.; Biswas, G.: Establishment of ecc-based initial secrecy usable for ike implementation. In: Proceedings of the world congress on engineering, vol. 1, (2012).

[11]. Ku, W.-C.; Chang, S.-T.: Impersonation attack on a dynamic idbased remote user authentication scheme using smart cards. IEICE Trans. Commun. 88(5), 2165–2167 (2005)

[12]. Wu, Z.; Gao, S.; Cling, E. S.; Li, H.: A study on replay attack and anti-spoofing for text-dependent speaker verification. In: Signal and information processing association annual summit and conference (APSIPA), 2014 Asia-Pacific, pp. 1–5, IEEE, (2014)

[13]. Liu, H.: A new form of dos attack in a cloud and its avoidance mechanism. In: Proceedings of the 2010 ACM workshop on Cloud computing security workshop, pp. 65–76, (2010)

[14]. Kumar, V.; Kumar, R.; Pandey, S.: Polynomial based noninteractive session key computation protocol for secure communication in dynamic groups. Int. J. Inf. Technol. 12(1), 283–288 (2020)

[15]. Sarvabhatla, M.; Reddy, M. C. M.; Vorugunti, C. S.: A robust remote user authentication scheme resistant to known session specific temporary information attack. In: 2015 Applications and innovations in mobile computing (AIMoC), pp. 164–169, IEEE, (2015)

[16]. Salem, M. B.; Hershkop, S.; Stolfo, S. J.: A survey of insider attack detection research. In: Insider attack and cyber security. pp. 69–90, Springer, Berlin (2008)

[17]. Alsalhi, I. N., Albermany, S. A.: Authentication of crns by using ban logic

[18]. Kilinc, H.H.; Yanik, T.: A survey of sip authentication and key agreement schemes. IEEE Commun. Surv. Tutor. 16(2), 1005–1023 (2013)

Cite this article as :

Rajesh Gundla, Sunil Gupta, C. Srinivasa Kumar, "A Three-Party Cloud Authentication Framework for Enhanced Security and Integrity", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 3, pp. 581-593, May-June 2021.

Journal URL : https://ijsrset.com/IJSRSET2310225