Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 3405-3411*

Research Article

A Survey on the security of Cloud Storage System

Guru Vimal Kumar M[a] ,Ragupathy P[b], Ramanan M[c]

[a] Assistant Professor, DepartmentofInformation Technology, Bannari Amman Institute of Technology,Sathyamangalam, Erode,Tamil Nadu
[b]Assistant Professor, DepartmentofComputer Technology, Bannari Amman Institute of Technology,Sathyamangalam, Erode,Tamil Nadu
[c]Teaching Assistant, Department of Physical Sciences & Information Technology,Agricultural Engineering College &Research Institute, Tamil Nadu Agricultural University, Coimbatore, India
[a] guruvimal09@gmail.com, [b] profragupathy@gmail.com, [c] pmramanan@gmail.com

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: Distributed computing is an emerging processing tool in software engineering today. Distributed computing is a collection of assets and services provided by a company or the internet. Different figuring approaches, such as matrix processing and dispersed registering, are broadened by distributed computing. Distributed computing is now used in both the modern and academic fields. Cloud encourages its customers by providing virtual assets through the internet. New procedures are emerging as the area of distributed computing expands. As the distributed computing environment grows, so do the security problems for cloud engineers. Since cloud clients save their data in the cloud, a lack of security in the cloud can jeopardise the client's trust. In this paper, we'll look at a few different aspects of cloud protection, such as multi-occupancy, versatility, and usability. We'll also look at current security strategies and techniques for a secure cloud. This paper will allow specialists and experts to consider the different security threats as well as the models and instruments that have been suggested.

Keywords: CloudSecurityStandards, Cloud Security,SecurityThreats,SecurityTechniques

1. Introduction

Internet figuring is also known as distributed computing. "Distributed computing is a model for empowering on-request and beneficial organisation admittance to a common pool of configurable registering properties," according to the National Institute of Standards and Technology (NIST)(e.g., networks, staff, stockpiling applications and administrations) that can be provisioned and distributed easily with minimal management effort or specialist co-op interaction[9]. For some, it is a worldview that provides computing assets and capacity, while for others, it is simply a method of accessing cloud programming and knowledge. Additionally, distributed computing reduces costs by allowing the organisation to share information. Associations should upload their data to the cloud so that their investors can access it. Google Apps is a good example of distributed computing. Regardless, the cloud provides a variety of services and benefits, but it does have some drawbacks in terms of data security and capacity. Several concerns related to cloud protection exist, including merchant lock-in, multi-tenancy, loss of power, administration disruption, data loss, and so on [3]. In this paper, we dissect the security concerns posed by the distributed computing model. The main goal is to consider different types of attacks and procedures in order to obtain the cloud model. Figure 1 illustrates the layers.

IaaS Assist from the foundation: There's no good excuse to purchase or manage server farm equipment (servers, stockpiling, organizing, and so forth)**SaaS**Programming as a Service: Complete applications with flexible internal constraints, addressing specific business needs, and a focus on end-client requirements.**PaaS**Stage as a Services: There's no valid need to directly manage OS, databases, and so on Programming interfaces for developing higher-level applications. Application segments that have been prefabricated.

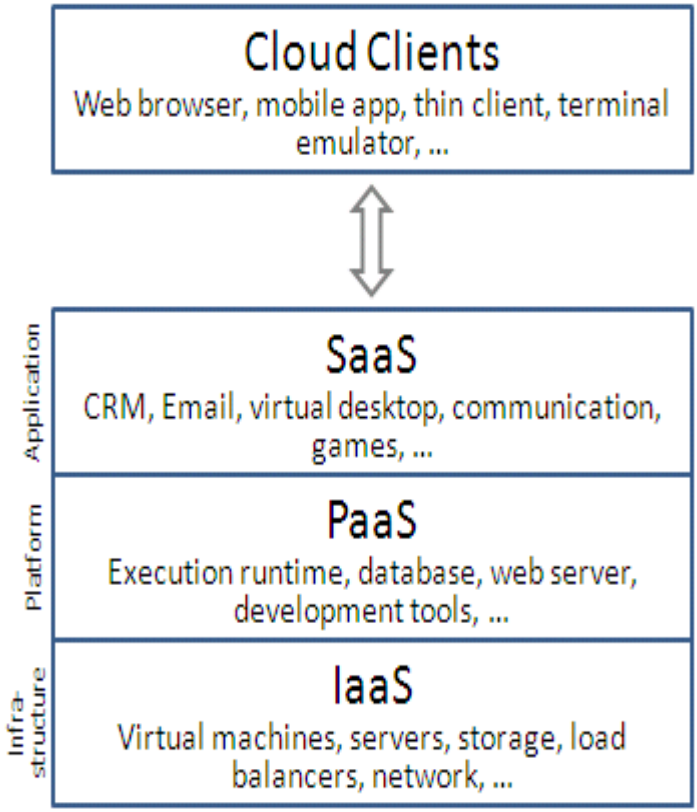

Figure 1. Layers of Cloud Computing

2. Cloud security issues

The organisation makes use of various cloud administrations such as IaaS, PaaS, and SaaS, as well as models such as public, private, and hybrid [6]. Different cloud protection problems exist in these models and administrations. Each assistance model is linked to a specific problem. Security problems are considered from two viewpoints. The first is from the viewpoint of a professional agency that ensures that the administrations they have are protected and also deals with the client's personal information. Another viewpoint is that of the customer, who ensures that the assistance they are receiving is properly reliable.

2.1 Elasticity

Flexibility is defined as a framework's ability to adapt to obligation changes by provisioning and disrupted assets in an autonomous manner, with the intention that the accessible assets coordinate the current interest as closely as possible wherever possible. Flexibility implies adaptability. Buyers may scale up or down depending on the situation, according to the document. This scaling allows occupants to use an asset that has already been assigned to another inhabitant. In either case, this may lead to classification problems.

2.2 Multi-tenure

A cloud model is used for a variety of purposes, including asset sharing, memory, stockpiling, and shared processing [2]. Multi-tenure allows for more efficient utilisation of assets while also lowering costs. It implies that different inhabitants living on the same physical/consistent stage at the supplier's premises share computational properties, administrations stockpiling, and applications. As a result, it disregards the confidentiality of information, resulting in data leakage and encryption, as well as an increase in the risk of cyber-attacks.

2.3 Loss of control

Cloud utilises an area straightforwardness model, allowing organisations to be unaware of the location of their administrations and data. As a result, suppliers can access their administrations from anywhere on the internet. In this case, the organisation may lose its details, and it is possible that they are unaware of the supplier's security instrument setup. Figure 2 illustrates this.

Figure 2. Loss of Control over Data

2.4 Insider assaults

A cloud platform is a multitenant oriented model that is managed by a single administration region for the supplier. This is a threat that arises from inside the organisation. For cloud jobs, there are no hiring guidelines or suppliers [1]. As a result, an outsider merchant will undoubtedly hack into the information of one organisation and either destroy or sell the information to another.

2.5 Data Loss

Since there are many occupants in the cloud, information integrity and confidentiality cannot be guaranteed. An organization's financial and customer tally losses can be caused by information loss. The refreshing and cancellation of information without any reinforcement of the information is a good example of this.

2.6 Network security

The practise of preventing and guarding against unauthorised intrusion into corporate networks is known as network protection. Endpoint security, which focuses on individual devices, is supplemented by network security, which focuses on how those devices communicate and the connective tissue that connects them.

2.6.1 Port examining:

A port is a location where data is exchanged. When a supporter plans a meeting, port examination takes place. Since port filtering is a natural part of web design, this exploits security concerns [5].

2.6.2 Man in center assault:

In this attack, the attacker creates an independent association and communicates with the cloud client on its private network, where the attacker has complete control.

2.6.3 Distributed forswearing of administration assaults:

Staff and companies are brought close an enormous amount of company traffic in a DDOS attack, and clients are denied access to a particular Internet-based service. [3]

2.7 Outsider assaults

This is one of the most disturbing issues in an organisation because it exposes the organization's confidential data. Mists despise private organisations because they have a greater number of interfaces than they do. As a result, programmers and assailants will take advantage of the API's flaws and potentially sever associations [1]. These assaults are less harmful than insider assaults because we are often unable to differentiate between the two.

2.8 Flooding Attack Problem

There are a number of employees in the cloud who communicate with one another and transfer data. The solicitations are prepared, and the listed occupations are validated first; however, this verification consumes a significant amount of CPU time and memory, and as a result, these workers are overburdened, and the offload is passed to another server[13].

2.9 Malware Injection Attack Problem

Since a large amount of data is transferred between the cloud provider and the purchaser in distributed computing, client confirmation and approval are needed [10]. When information is transferred between the cloud provider and the client, the assailant may insert vindictive code. Following that, the first client may be required to wait before the work that was maliciously presented is completed.

3. Techniques in Cloud Computing

3.1 Data Encryption

If you want to store sensitive data on a large data store, you'll need to employ data encryption techniques. Passwords and firewalls are appropriate, but individuals may circumvent them to gain access to your data. When data is scrambled, it is stored in a structure that cannot be read without an encryption key. To the gatecrasher, the knowledge is completely useless. It is the process of converting knowledge into a secret code. If you want to read the scrambled information, you'll need the mysterious key or hidden phrase, which is also known as the encryption key.

3.2 Authentication and Identity

Different methods are used to confirm clients and even transmitting systems, but cryptography is the most commonly known [8]. Server validation may be done in a variety of ways, such as using passwords that are identified independently, using a security token, or using a quantifiable number like a unique mark in the framework[7]. When the project uses many cloud specialist co-ops (CSPs), there is a problem with using traditional personality methods in a cloud environment[14]. Personal data synchronisation with the venture isn't adaptable in this use case. When shifting foundation toward a cloud-based arrangement, various issues arise with traditional character approaches. The data security is shown in figure 3.

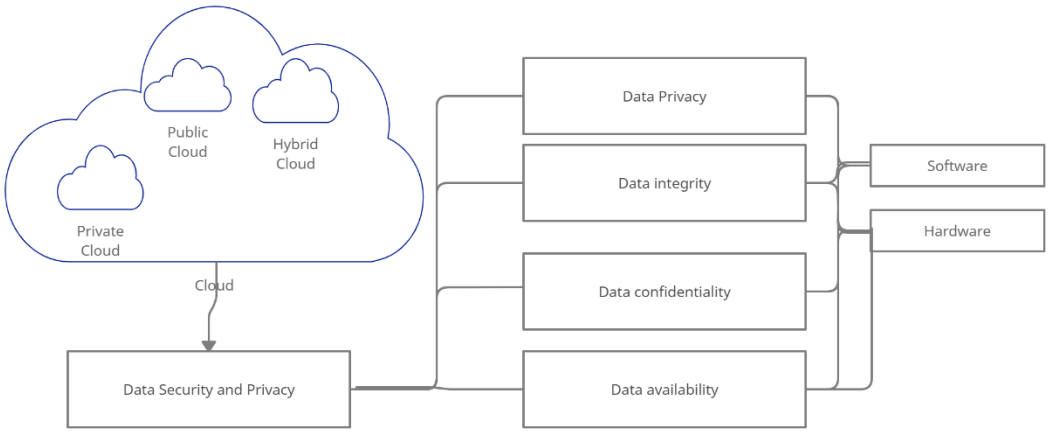

Figure 3: Data Security in Cloud

3.3 Availability of Information(SLA)

In distributed computing administrations, data or knowledge not being accessible is a major problem. The Administration Level Understanding is used to provide information on whether or not the organization's assets are available to clients. It is a relationship of confidence between the customer and the supplier [2]. One way to ensure asset accessibility is to have a backup plan in place for surrounding properties, just as you would for the most critical data. This gives the client access to asset data even though the assets are inaccessible.

3.4 Information uprightness and Privacy

Data and assets are distributed to legitimate clients using distributed computing. Internet browsers can access assets, and pernicious aggressors can access assets as well [18]. Giving mutual trust between supplier and customer is a helpful solution to the issue of data integrity. Another option is to include legitimate confirmation, approval, and bookkeeping controls, so that the path to data is subjected to several layers of verification to ensure proper asset utilisation [4]. Some access instruments, such as RSA endorsements and SSH-based passages, should be given.

3.5 Malware-infusion assault arrangement

This setup creates a number of customer virtual machines and stores each one in a central repository. It makes use of a virtual working environment called FAT (File Allocation Table)[10]. The FAT table contains the programme that is managed by a consumer. Hypervisor is in charge of overseeing and planning all of the events. For honesty checks, the IDT (Interrupt Descriptor Table) is used.

3.6 Flooding Attack Solution

The staff in the cloud are collectively referred to as an armada. For framework style demands, one armada of workers is considered, one for memory the board, and the last one for centre calculation related positions. Both of

the staff in the armada can communicate with one another. When one of the employees becomes overburdened, another worker is brought in to take his or her place, and this new worker, known as the name worker, has all of the current worker statuses and can be used to update objections and states. Hypervisor can be used to supervise work[12]. Hypervisor is also in charge of job clearance and confirmation. PID may be used to identify a solicitation from an authorised customer. The PID can be scrambled using RSA as well.

3.7 Secure Information Management

It is a data security procedure for storing a variety of data in a central repository. It includes specialists who operate on frameworks that need to be examined and then submit data to a worker known as the "Security Console." The protection system is managed by an administrator, who examines the data and takes action in response to any alarms. As the cloud client base, reliance stack, and cloud protection systems to resolve security issues develop, cloud security becomes increasingly complicated across the board. It's sometimes referred to as Log Management. Security standards such as PCI DSS and SAS 70[2] are also provided by cloud providers. Another model of Information Security Management System is Data Security Management Maturity. Figure 3 illustrates this.

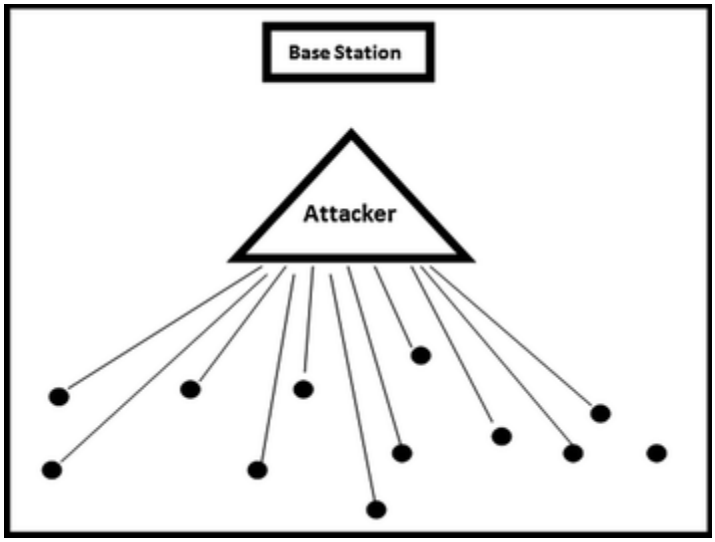

Figure 3 . Flooding Attack arrangement

4. Security Standards in Cloud

The methodology and cycles for executing a security programme are defined by security principles. To maintain a stable environment that provides privacy and security, some specific advances are made by implementing cloud-related exercises in accordance with these standards. In the cloud, a concept known as "Safeguard in Depth" is used to provide protection [3]. This concept has many layers of security. As a result, if one of the mechanisms fails, the covering technique may be used to provide protection since it has no single point of failure. Endpoints typically have a security policy in place, with access controlled by the client.

4.1 Open Authentication (OAuth)

It's a method for collaborating on data that's been checked. It is primarily used to grant engineers access to knowledge. Clients can grant engineers and buyers access to data without revealing their identities [3]. To be honest, OAuth doesn't provide any protection without the help of others; instead, it relies on different conventions, such as SSL, to provide security.

4.2 Security Assertion Markup Language (SAML)

SAML is primarily used in business transactions to ensure safe communication between online partners. It is an XML-based standard that is used for partner verification and approval. The head (a client), the specialist co-op (SP), and the personality supplier (IDP) are the three jobs identified by SAML [11]. In XML design, SAML provides questions and reactions to indicate client credits approval and validation data. The mentioning group is a website that collects security information.

4.3 SSL/TLS

TLS is used to provide encrypted communication over TCP/IP. TLS is divided into three stages: In the first step, customers make arrangements to determine which codes will be used. For validation in the second level,

main trade calculation is used [3]. These are public key estimates for key trade calculations. Message encryption and code encryption are used in the final and third stages.

4.4 OpenID

SSO (single sign-on) is a technique used by OpenID. It is a standard login procedure that allows clients to log in once and then use all of the participating systems [16]. It is not based on central approval for client validation. The table 1.1 describes comparative analysis for existing security schemes.

Table 1.1 Comparative Analysis for Existing Security schemes

S.No	Security schemes	Merits	Demerits
1.	Ciphertext-Policy Attribute Based Encryption (CP-ABE) [10]	Expressive effective	Security issue
2.	Ciphertext-Policy Attribute Based Encryption (CP-ABE) [15]	Effectively solving the problem of user retracting	Computation expense
3.	identity-based proxy-oriented data uploading and remote data integrity (ID-PUIC) [17]	Secure System	Computational complexity of the Diffie-Hellman problem
4.	Remote data integrity checking schemes based on PKI [18]	Decreasing the complexity of the system	Malevolent cloud attacks
5.	Identity-based Cloud Data Integrity Checking (ID-CDIC) protocol[19]	Security high	Complexity
6.	Division and Replication of Data in the Cloud for Optimal Performance and Security[2]	To tackle both security and the performance issues	Computationally expensive

5. Conclusion

This paper depicts some cloud concepts and demonstrates cloud properties such as adaptability, stage-free operation, minimal effort, versatility, and unwavering consistency. While there are numerous security problems in distributed computing, we have examined a few of them in this paper, as well as techniques to avoid them. These strategies can be used to maintain secure communication and mitigate security issues. This analysis focuses on all of the problems, such as attacks, knowledge misfortune, and unauthenticated access to information, as well as the solutions to address those issues. The traditional security arrangements provided by cloud climate do not plan well to its virtualized surroundings because distributed computing is complex and perplexing. Cloud Security Alliance (CSA) and NIST, for example, are working to improve distributed computing security. We've discussed a few different security methods in this article, but there are also a few different methodologies that are being used at the same time. A few standards are also proposed that can be used to maintain stable communications and protection in a cloud where various frameworks communicate and perform tasks.

References

Abbas,SalimAli,2015, “Enhancingthesecurityofidentityandaccessmanagementin cloud computing using elliptic curve cryptography”. Int. J. Emerg. Res. Manag.Technol.4(7).

Ali, M., Bilal, K., Khan, S., Veeravalli, B., Li, K., &Zomaya, A. (2015, “ DROPS: Division and Replication of Data in the Cloud for Optimal Performance and Security”, IEEE Transactions on Cloud computing.

Behl,Akhil,Behl,Kanika,2012, "Securityparadigmsforcloudcomputing" In:ProceedingsofFourthInternationalConferenceonComputationalIntelligence,CommunicationSystemsandNetworks(CICSyN).IEEE,pp.200–205.

Cao,Ning,Wang,Cong,Li,Ming,Ren,Kui,Lou,Wenjing,2014, "Privacy-preservingmulti-keywordrankedsearchoverencryptedclouddata", In: ProceedingofIEEETransactionsonParallelandDistributedSystems,Vol.25,Issue1,pp.222–233.

Fan,Haolong,Hussain,FarookhKhadeer,Younas,Muhammad,Hussain,OmarKhadeer,2015,"Anintegratedpersonalizationframeworkforsaas-basedcloudservices", FutureGener.Comput.Syst.53,157–173.

Guru Vimal Kumar M, and A.C.Kaladevi "Optimized Load Balancing in Clouds Using Bee Colony Algorithm" in Australian Journal of Basic and Applied Science(AJBAS), 9(6) special 2015 ISSN:1991-8178, Pages:16-19

Guru Vimal Kumar M, and U.S.Ragupathy "A Survey on Current Key Issues and Status in Cryptography" in the IEEE International Conference on Wireless Communications, Signal Processing and Networking (WISPNET) held at SSN College of Engineering, Chennai, India, during 23-25 March 2016

Guru Vimal Kumar M, and U.S.Ragupathy "Performance analysis of image steganography using wavelet transform for safe and secured transaction", Multimedia Tools and Applications, Springer, Vol. 79, no. 13-14, pp-9105-9115, April-2019

Kim,Jin-Mook,Moon,Jeong-Kyung,Hong,Bong-Hwa,2013, "AnEffectiveResourceManagementforCloudServicesusingClusteringSchemes".

Li, J., Yao, W., Zhang, Y., Qian, H., & Han, J. (2017). Flexible and fine-grained attribute-based data storage in cloud computing. IEEE Transactions on Services Computing, 10(5), 785-796.

Liu,Qin,Wang,Guojun,Wu,Jie,2014.Time-basedproxyre-encryptionschemeforsecuredatasharinginacloudenvironment.Inf.Sci.258,355–370.

Modi, Chirag, Patel, Dhiren, Borisaniya, Bhavesh, Patel, Avi, Rajarajan, Muttukrish-nan, 2013. A survey on security issues and solutions at different layers of cloudcomputing.J.Supercomput.63(2),561–592.

Nabil,Sultan,2014, "Makinguseofcloudcomputingforhealthcareprovision:op-portunitiesandchallenges", Int.J.Inf.Manag.34(2),177–184.

Sumitra, B., Pethuru, C.R., Misbahuddin, M., 2014. A survey of cloud authenticationattacksandsolutionapproaches.Int.J.Innov.Res.Comput.Commun.Eng.2(10).

Yang, K., & Jia, X. (2014). Expressive, efficient, and revocable data access control for multi-authority cloud storage. IEEE transactions on parallel and distributed systems, 25(7), 1735-1744.

Younis,YounisA.,Merabti,Madjid,Kifaya,Kashif,2013, "SecureCloudComputingforCriticalInfrastructure:ASurvey",LiverpoolJohnMooresUniversity,UnitedKingdom,Tech.Rep.

Wang, H., He, D., & Tang, S. (2016). Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud. IEEE Transactions on Information Forensics and Security, 11(6), 1165-1176.

Yu, Y., Xue, L., Au, M. H., Susilo, W., Ni, J., Zhang, Y., ... & Shen, J. (2016). Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Generation Computer Systems, 62, 85-91.

Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2017). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, 12(4), 767-778.