Vol. 03, No. 4,(2019),182–192, **ISSN:2581-3242**

IJMLNCE JOURNAL

International Journal of Machine Learning and Networked Collaborative Engineering

Journal Homepage: http://www.mlnce.net/home/index.html

DOI : https://doi.org/10.30991/IJMLNCE.2019v03i04.001

A Survey of Cloud Computing Security Issues

[a]Priyanka Singh, [b]Manju Khari,

[a,b]*CSE, AIACTR, Geeta Colony, Delhi, India*

[a]*priyankasingh.singh193@gmail.com*

[b]*manjukhari@yahoo.co.in*

Abstract

In the world of computer networking, cloud computing makes a technical shift of computing services being provided locally to being provided remotely by third-party service providers. The data which was previously retained by the control of users now it's under the control of service providers. Cloud computing conveys numerous economic and practical assistances along with severe security alarms that might impend commercial endurance and business status. The cloud computing definition is still not clear in a huge portion, as of the extent of security threats and the large expanse of virtual information being distributed over the unsecured area. This manuscript aims to assess in what way security risk issues are affecting the surviving and eventual cloud platform. This survey examines the published resources and studies, examines available concerns laterally with existing countermeasures to assess the complete assertion level of security of the cloud. The primary goal of the survey is to analyse the security risks and the existing security algorithm's performance in terms of different security parameters. This study includes the basics of cloud computing by adding its characteristics, models, and their categories. The analysis also embraced the existing security concerns faced by researchers and their imposed methodologies.

Keywords

Cloud Computing,

Security Issues,

Security Risks,

Security Methods

1. Introduction

1.1 Defining Cloud Computing

Cloud Computing is a kind of outsourcing of computer programs. The term "The cloud" is a phrase for the internet. Using cloud computing, users can access software and applications from wherever they are; the existence of computer programs held through some external party, and is located in the cloud. It comprises that consumers do not need to concern about equipment for example power and storage; they can just appreciate the finale result. Outmoded commercial applications have constantly remained very complex and costly. The extent plus range of hardware and software requisite to track them are frightening. It requires a whole squad of professionals to set up, organization, assessment, run, protected, and bring up-to-date them. By the use of cloud computing, it eliminates those problems that come with storing your specific data, because you're not handling hardware. The shared infrastructure means it works like a utility: You only pay for what you need, upgrades are automatic, and scaling up or down is easy. Virtualized assets are used to access applications and distributed services in cloud computing. Two core concepts of the cloud are abstraction and virtualization abstraction means to hide details of storage, system implementation from users.

Virtualization refers to the process of creating virtual data centers in the cloud which provide scalability and use of resources in a cloud environment. In a cloud computing environment, an entity that works within an organization is Cloud Service Provider (CSP). CSP manages all the services and applications provided by cloud computing. The most challenging aspect for an organization is data storage and data transmission over the cloud in a secure manner. To achieve data security the data storage and data transmission should be in encrypted form by using different crypt algorithms. Cloud storage associated with some of the vulnerabilities related to data confidentiality, data integrity, and data availability. To provide better security in the cloud we should consider the risks associated with cloud storage and transmission.

Section 1 is organized as follows in Section 1.2 characteristics of the cloud is discussed. Section 1.3 discusses cloud services and models. Section 2 comprises issues related to the security and privacy of cloud data. Section 3 includes a literature survey. Comparative analysis of security imposed in cloud computing is shown in Section 4 and the whole survey is concluded in Section 5 with the future scope.

1.2 Characteristics of cloud

Cloud computing provides appropriate, on-demand service access with pooled configurable computing assets which can be (systems, servers, storage, applications, and facilities) that might be promptly released and provisioned with nominal administration strength or service provider interface. Being a service provider of cloud computing doesn't mean just adding IT properties, it means providing tactical, essential information technology. This cloud model is composed of five essential characteristics [1].

1.2.1 Provide On-demand resources:An end-user can unilaterally provision computing competences, for example, server period and storage of network, as desired spontaneously deprived of requiring consumer collaboration with every cloud service provider (CSP).

1.2.2 Wide network access:The cloud competencies are widely accessible above the network also retrieved over and done with standard mechanisms that endorse usage through various thin or thick customer raised areas (e.g. tablets, laptops, cell phones, and terminals).

***1.2.3 Resource pooling*:** Computing resources provided by service providers are pooled together to oblige several clients with a multi-tenant prototypical, thru dissimilar virtual and physical resources vigorously allocated and reallocated as per the demand of the customer. There must be the wisdom of location freedom as the consumers usually take no control or awareness over the particular site of the delivered assets nevertheless might be capable to stipulate location by an advanced level of generalization (such as., nation, public, or datacentre). Illustrations of assets comprise storage, handling, memory, and network bandwidth.

1.2.4 Swift elasticity: The capabilities can be provisioned and released elastically and some cases comprise spontaneously, to measure swiftly apparent and hidden adequate with demand. Towards the user, the provisioning of abilities offered unlimited and can be adapted to any extent at every time.

***1.2.5 Pay-per-usage services*:** A Cloud structure spontaneously regulatesand improves resource use for metering capability at selected level of generalizationsuitable to the sort of package (e.g. storage, processing, bandwidth, and active customer accounts). Resource practice can be examined, measured, and informed, providing pellucidity for the provider and user. These characteristics are used by the different service models of cloud which provide services as per user demands. The next section covers all the services provided by cloud systems.

1.3 CLOUD SERVICES AND MODELS

1.3.1 Cloud computing as a service

Cloud computing used as a service to its clients and introduced its services through different service models. The models of cloud computing such as software, platforms, and infrastructures available as services of the web over the Internet, and clients of these services are unaware of the physical place of wherever these services are executed. The businesses get hardware and software assets as services from the providers. Cloud

computing defines differently by each organization and service provider. E.g. "a prototype for permitting abundant, suitable, on-demand system access to a pool of shared configurable resources of computing (for example, servers, storage, network, services, and applications) which can be quickly released and provisioned by least efforts of management or interaction of service providers" defined by the National Institute of Standards and Technology (NIST) [1]. Buyya, Broberg, and Gościński stated that the cloud computing services distributed into three modules such as Software as a Service SaaS, Infrastructure as a Service PaaS, and Platform as a Service PaaS, the management tools and content of these services is better illustrated in figure 1 [2].

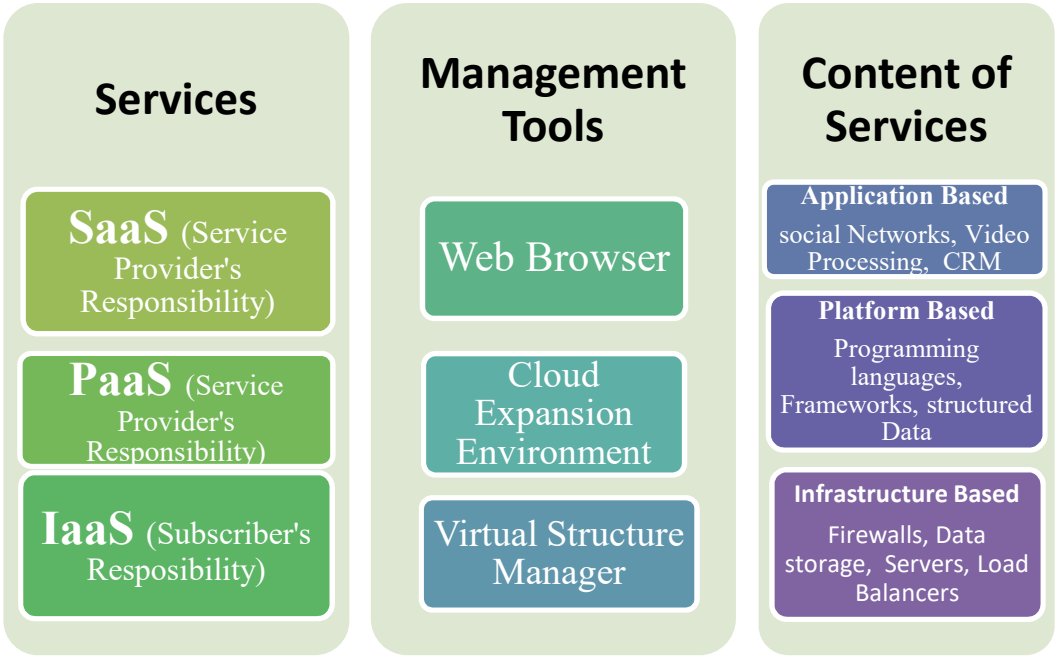

Figure1. Services of Cloud Computing

1. Software as a Service (SaaS)

SaaS model also refers to as a service-oriented model. It works on a pay-per-usage basis and provides two types of services which are application and process-oriented services. In this model to access the applications through various client devices, a program interface can be used. The infrastructures such as operating systems, servers, networks, and others are not managed or controlled by the consumers. Content of services provided by SaaS is all application-based which includes social networks, video processing, CRM, and the web browser used as the management tool.

2. Platform as a Service (PaaS)

Independent platforms besides each kind of supports is provided by this model to all the consumers, testers, designers, and developers and don't allow interfering with other platforms. It also provides an atmosphere wherever applications stay prepared to develop and installed. The clients of cloud consume the delivered platform, for instance, programming languages and Oracle-based databases, deprived of disturbing about the essential information like the configuration and needs of hardware and software.

3. Infrastructure as a Service (IaaS)

IaaS contains properties of scalability and elasticity also provides support such as operating system, storage, and networking. This cloud service is used by the consumers where they can deploy and run arbitrary software which can include operating systems and applications. With the underlying cloud infrastructure the consumers have control over the deployed operating system, application, and storage

however the cloud base is not controlled by the customers. This service provides raw computing, storage, and operating services where cloud users can build customer service and application.

The next section illustrates the deployment models of cloud which have been classified by the NIST and divided into four types of models such as public, private, community, and hybrid cloud models.

1.3.2 Cloud deployment models

The cloud services and deployment is an important aspect of cloud computing. These services are deployed in different infrastructures to provide a better platform for cloud users as per their requirements. This has been classified by dividing the cloud infrastructure into different classes. These strategies provide a baseline for how to best use cloud computing [3].

1. *Public Cloud Model*

Public clouds can be used and accessible by all cloud users. It provides scalability and resource sharing. The public cloud is controlled and operated by CSP and provides services to users via the internet. for example social networking websites, most of the Google services.

2. *Private Cloud Model*

This model of cloud computing provides a distinct and secure cloud-based environment that can be operated by specified users only. It doesn't allow any unauthorized access and managed by the organization or third party users. Most of the companies host their private reserved clouds which are accessible merely through the internal users of the company. Private clouds enhance the confidentiality of data by creating facilities available solitary for interior customers. For example Amazon virtual private cloud.

3. *Community Cloud Model*

The services of this model are provided by organization communities having common interests and needs. They work in a multitenant environment and managed or controlled by either organization or CSP. For example Google Apps for the government like all the police stations inside a province working a particular cloud designed for distributing logs with a single pursuit boundary used through all police stations.

4. *Hybrid Cloud Model*

This cloud platform is a composition of two or more clouds such as (private, public, community clouds). It provides the clustering of different resources also enables application and data portability. The concept of hybrid is preferred predominantly for cost efficiency besides scalability. E.g.: an organization keeping all its confidential figures interior and outsourcing added non-critical loads towards public clouds.

The use of all the services provided by the cloud makes the user more concerned about their security. The more data is shared over the different platforms of cloud increase the chance of data breach during transmission and storing. The security and privacy issues are detailed in the next section.

2. Issues Related to Security and Privacy of Cloud Data

As per concern above the security of cloud keeps growing, this one has to turn out to be precarious for providers of cloud services to exist and validate their capability to defend consumer data. The supreme mutual resources to achieve this are to acquire reliable safety authorizations and inspections for potential businesses.

2.1 Data Confidentiality issues

Confidentiality refers to make the data or information of a user confidential and does not allow the unauthorized disclosure of information. The CSP of a cloud environment has the responsibility to make the user's data confidential and provide protection from disclosure to unauthorized users or intruders but in some cases CSP itself contains some untrusted or dishonest members who can view and make an unauthorized alteration in the user's confidential or private data [4]. The main issues related to cloud data confidentiality are:

2.1.1 *Multi-Tenant Platform*: The major issue in a cloud environment because it works on a multi-tenancy

model where the number of similar devices is shared among the multiple independent users and this may lead to the accessibility of data to all the cloud users. This environment opens up data stealth possibilities.

2.1.2 ***Insecure APIs*****:** When the cloud users deploy their data on the cloud every CSP generates an API for reference. API's contain all the design and architectural related details of cloud users that can be accessible by attackers who can design different attacks by using that information.

2.1.3 ***Leakage of Data:*** Customer's data stored on cloud away from their location and the second concern is data moving to a multi-tenant environment that may lead to data leakage to the third party user or attackers.

2.2 Integrity related issues

In a cloud, environment integrity implies that the data should be securely stored on cloud servers that cannot be compromised or altered by any malicious users or service providers. Any delete or update operations by the unauthorized user lead to losing the integrity of data. Since the cloud data is shared via the internet or accessed by web browsers so the web-based attacks are more prone to change the data integrity. Cross-site scripting, SQL injection and Spoofing attacks are some examples of attacks that occur due to loss of integrity.

2.2.1 ***Data Manipulation*****:** It violates the accuracy and correctness of user data by altering or manipulating it. Cloud users store their data on cloud servers that can be accessed rarely and the cloud servers are shared by all that results in the data may be modified maliciously. The accidental errors made by administrators make the adversaries design attacks over the servers.

2.2.2 ***False computation on remote servers*****:** Due to the hidden computation details to the cloudusers it is hard to judge the computation executed with good integrity and it may lead to false computation results and unfaithful server's storage [1].

2.2.3 ***Cloud data outsourcing*****:**Itis done at the CSP end that leads to threats for integrity. It can delete or modify the part of the user's data and this fact cannot be detected by the users even when it is sent incomplete to the client it remains undetected.

2.3 Availability related issues

Enterprises that offer cloud services must provide on-demand availability of data to their cloud users. It is a major concern of cloud security but availability to third party users may lead attacks.

2.3.1 ***Distributed denial-of-service DDOS*****:** Distributed denial of service (DDOS) attack caused the unavailability of data to the clients. The attacker compromises the system and sends a huge amount of ambiguous requests to the cloud server. In some cases, CSP itself supports attackers in letting the system resources compromise.

2.3.2 ***Easy accessibility of cloud*****:** It leads to available services and resources to all the cloud users due to its multi-tenancy feature this may open the opportunity to attackers for data compromise.

Several security issues that most of the cloud users consider being concerns or serious concerns. Most prominent concerns were related to being fully dependent on a cloud service provider. This may lead to raising the number of risks; the next section presents some of the risks related to security issues.

2.4 Risks occur while using cloud services

As all the cloud usersarereliant on a cloud service provider's security assertions and observes is added security fear. Leading, insufficientcontrols of security provided by cloud service provider mightthreaten the security principles as confidentiality, integrity, and availability of assistancedata. Moreover, abandonin resistor to the cloud service provider mighteffect in harm of authority and corporealcontroller over registered documents and data [5]. Significant security consideration is essential in six addedexplicitregions of cloud computing

2.4.1 Security when data in transit.

When data is in motion or actively moving from one location such as from a local storage device to a cloud storage device is considered to be less secure. When traveling via a network to network or through internet effective data protection measures for in-transit data are critical.

2.4.2 Security when Data at rest

Data at rest is inactive data and this data is not moving from one device to another or one network to others. It is considered that the data which is stored on networks or any devices at rest is less vulnerable than data in transit but still attackers find it a more valuable target to attack.

2.4.3 Cloud legal and regulatory issues.

When the cloud service provider cannot provide their compliance evidence with the relevant requirements or does not permit audits by the cloud then the investment of customer's in achieving certification is lost. These legal and regulatory issues are considered to be a great risk for customers.

2.4.4 Robust separation between data belonging to different customers.

If the separation control fails it may lead to data leakage. This failure can be used by an attacker to gain access from one organization's resource to another user's or organization's assets or data.

2.4.5 Authentication of users/processes/applications.

Malicious actions of insiders who are working in the organizations can cause damage. These activities can be performed by either or both customer organization or provider organization. When the authentication is not properly monitored by providers leads to risk.

2.4.6 Incident Response.

When there is a lack of control over detection, reporting, and subsequent management of data breaches by the cloud provider then these incidents impact the customers and it may lead to a great risk for the providers and customers.

These risks and security parameters are considered by some of the researchers in their researches. Some of the techniques, methodologies proposed by recent researches are discussed in the next section to improve the security risks by several cryptographic schemes.

3. Related Studies

Data security in cloud computing using Hierarchical CP-ABE (cipher text policy based attribute-based encryption) technique for the access control defined in document [6] by using RSA and Blowfish algorithms for data encryption and decryption to maintain data confidentiality. Hierarchal CP-ABE encrypts all attributes which are assigned to users to provide integrity of data. This approach provides scalability and flexibility for access control and prevention from SQL injection attacks. This approach removes the limitations of scalability and flexibility of existing CP-ABE based policy.

Paper [7] discovers Byzantine fault tolerance algorithm with AES algorithm. A three layer system structure model is used in their proposed approach first layer designed as OTP authentication module for cloud user authentication and user permission, second layer manages the encryption of user’s data by AES algorithm and the third layer designed for faster data recovery by using Byzantine fault tolerance algorithm. This approach ensures the security of data at each layer.

Hybrid Improved cipher block chaining with Genetic algorithm encryption security service. Authors in [8] detailed in their approach that multiple keys are used and one key generation by hybridization improved cipher block chaining and another with genetic algorithm. This approach fulfill three objective of minimum execution time, reduction in storage space by converting content into binary form and better encryption security by hybrid Improve block chaining with GA.

A model for authentication and multi-tenancy related threats of cloud computing is proposed by using ECC (Elliptic Curve Cryptography) and used Kerberos authentication protocol to improve the authentication

security. They have studied multi-tenancy issues related to each cloud model such as PaaS, IaaS, SaaS. This model also introduced a Resource allocation manager based unit system model (RAMU) for protection from multi-tenancy issues and authentication of users by using five step model of resource allocation [9].

Hybrid encryption algorithm for data security in cloud a hybrid algorithm used the two existing algorithms RSA and AES. The objective of their research was secure upload, secure download of data and secure usage of encryption keys over the cloud. Approach proposed by authors in [10] used 1024 bits of RSA and 128 bits of AES so private key cannot be guessed and hybrid algorithm approach enhance the security of text files and for uploads or downloads required private key that cannot be guessed by intruders due to high security feature of Hybrid algorithm.

In [11] research describes the speed of RSA algorithms increased by using multithreading scheme on latest multicore CPU's. In this approach the encryption and decryption done as per the number of blocks. The multithreaded approach reduced the complexity of computation and enhances the speed of RSA. This model compares the encryption time of sequential and parallel models, this approach also showed that the multithreaded or parallel model is more effective and reduced computation cost.

Inter cloud communication by using RC6 and AES algorithm researched by [12] demonstrates their flexibility in secure transaction over cloud. This approach is an efficient secure framework of user cloud. Their experimental results show that the idea they have used is superior in relations of key randomization, by means of private key and offers good provision to cloud server to consumer, user to user and user to cloud server.

In [13] authors developed an approach of RSA algorithm of advancedefficacy and TPA meant forvalidation of the files which executeoperation over cloud. Added, they also use the digital signature arranged that TPA to validate the source and moreoverrelate on the HMAC utility for hashing the value of key over the cloud. The tentativeoutcomes proved that digital signing algorithm and RSA is extraeffective than former signature algorithm.

In paper [14] authors focused on the integrity authentication for outsourced information over the cloud. They merge the encrypting mechanism alongside by integrity authenticationapproach. They used an asymmetric and hashing cryptographic algorithm. This paper proposed an ElGamal encryption algorithm and SHA- 256 (SHA-2) hashing algorithm. These are used for guaranteeing data storage precision on untrusted server.

Paper [15] gives an idea of Virtual Machine migration framework centered on hash based validation code and Diffie-Hellman key exchange procedure for authentication. Their work confirmed the frame consuming security investigation. Adding up, the recommended framework they have used is a protected and efficient process to VM Migration in a two-party relocation model.

The data security problem of hospital cloud database is solved by introducing a P-AES algorithm in literature [16]. The P-AES algorithm is improved version of AES algorithm with high efficiency. This algorithm is successfully applied on the information system database of hospital and with the experimental results it proved that the P-AES algorithm has the greater efficiency of encryption and decryption compared to previous AES algorithms and suitable for processing of long data. While hybrid algorithm provides the security and protection to the data which is stored at the medical cloud database and also improve the privacy of patient's information. With this great idea of P-AES algorithm it has some limitations too with Encrypting only text data cannot apply on data such as images, pictures or videos and can only encrypt data using 128 bit key. Data privacy and data utility has the major role in processing huge data in cloud platforms that attracts the infrastructure which support big data applications.

Document [17] implements a model of anonymization based on privacy preservation using K-anonymization criteria and combining Grey wolf optimizer and cat swarm optimization (GWO-CSO) algorithms for the preservation of privacy in big data before sending it to cloud. This research protects the privacy of users with proper data utilization with optimization based algorithms which improve the performance of anonymization based algorithms. The user data is saved in K-anonymized database and requests are processed to collect records from original database. The records are analyzed to hide the information for better privacy and are categorized using K-anonymization criteria then GWO-CSO algorithms are applied for constructing K-anonymized database where K duplicate records are created within

original database. So this approach provides accuracy in maximum classification with minimum data loss and more data privacy.

4. Comparative Analysis of Security Imposed in Cloud Computing

Cloud computing provides its services to users via service delivery models but this cloud platform and its delivery services are exploited by attackers. This may violate the data security and privacy of cloud platform , by focusing on these exploitations different security methods made by using existing security, key exchange algorithms. For example the cloud communication is protected by using secured key exchange algorithm RC6 and data has been protected through AES algorithm [12]. The privacy of user has been protected by optimization based algorithm [17]. The hybrid of data encryption algorithms and key exchange algorithms has been contributed in existing data protection schemes. The recent security ideas are summarized in (table 1) and a comparative analysis is made on the bias of used algorithms, security parameters and related issues. Table 2 shows the comparative analysis of imposed security algorithms on the basis of different parameters such as security, time complexity, flexibility and privacy.

Table 1: Comparative Analysis of Existing Security Methods

Researched By	Idea	Related Algorithms	Security parameters	Issues Covered
VishakhaM. Shelke,John Kenny [6]	Hierarchical CP-ABE	RSA and Blowfish	Confidentiality Integrity Authorization	Scalability & Flexibility of data
Navia Jose, Clara Kanmani A [7]	Byzantine fault tolerance algorithm	AES	Authentication	Data recovery
MahalakshmiJeyabaluy, KuppusamyKrishnamoorthy[9]	Hybrid Improved cipher block chaining with Genetic algorithm	Genetic Algorithm and Hybrid Algorithm	Integrity Confidentiality	Space Complexity Time complexity
HimelDey, RifatAslam, HossainArif [11]	ECC and Kerberos protocol, RAMU	ECC algorithm	Authentication Availability integrity	Multi-tenancy
Vishwanath S Mahalle, Aniket K Shahade [8]	Hybrid Encryption Algorithm	RSA and AES	Authentication Confidentiality Integrity	Security during upload/download of files
Purnima Gupta, Deepak kumarverma [10]	Multithreading scheme	RSA	Confidentiality	Computation Complexity, Encryption Time
Bhute&Arjaria [12]	Secure inter cloud communication	AES and RC6	Confidentiality integrity	Flexibility in inter cloud communication
Patel and Patel [13]	RSA higher efficiency algorithm and TPA	RSA, TPA, HMAC function	Authorization Authentication	Improve authentication using HMAC with

			integrity	TPA
Panimalar&Subhashri [14]	ElGamal encryption algorithm and SHA-256 (SHA-2)	SHA hashing algorithm	Integrity Authentication Availability	Data storage correctness and integrity verification
Majhi [15]	Authentication in Virtual Machine migration	Diffie-hellman and HMAC	Confidentiality Authentication Integrity	Improve VM migration
Fenghua Zhang et. al. [16]	P-AES algorithm and Hybrid Algorithm	AES and RSA	Privacy Confidentiality	Improve privacy and time complexity for encryption and decryption
SumanMadan&PuneetGoswami [17]	(GWO-CSO) algorithms and K-anonymized database	Grey wolf and Cat Swarm optimization algorithms	Data privacy and data utilization	Maximum classification accuracy and privacy with minimum data loss

Table 2. Comparision between imposed security algorithms

Different Parameters	**AES**	**RSA**	**Blowfish**	**ECC**	**RC6**	**SHA**	**Optimization algorithm**
Confidentiality	✔	✔	✔	✕	✔	✕	✕
Integrity	✔	✔	✔	✔	✕	✔	✕
Availability	✕	✕	✕	✔	✕	✔	✕
Authentication	✔	✔	✔	✔	✕	✔	✔
Authorization	✔	✕	✔	✕	✔	✕	✔
Time Complexity	✕	✕	✔	✕	✔	✕	✔
Flexibility	✔	✕	✔	✕	✕	✕	✔
Privacy	✔	✕	✕	✔	✕	✔	✕

5. Conclusion and Future Scope

Cloud computing comprises facilities for users through the effective employment of shared resources. Despite its effectiveness for cloud consumers along with cloud service providers, its occurrence is slowed down by numerous security issues. This paper extant a short survey of security issues, risks, and literature contributions directing at the security of the cloud. These security issues embrace cloud data security and cloud services. We also study the security methodologies used by the researchers and analyze their contribution in terms of idea used, imposed algorithms, security parameters, and covered security issues. Moreover, a comparison among the imposed key exchange and cryptographic algorithms made to analyze their effects based on parameters as security, time, flexibility, and privacy. We also investigate that a large number of privacy and security algorithms, intrusion detection techniques require agreement by CSP. Our future research would be based on the classification of attacks based on virtual machines, storage, network, and application. It will be motivating to investigate all the related countermeasures and limitations. We will also explore different intrusion or threat detection models.

References

[1]. ShrutiChabbra, V.S. Dixit "Cloud Computing: State Of The Art And Security Issues." *ACMSigsoft Software Engineering Notes*, Volume 40, March 2015

[2]. Mell P.M. and Grance.T "The NIST Definition of Cloud Computing." *In Computer Security Publications from the National of Standards and Technology (NIST)* , 2011.

[3]. Buyya, Rajkumar, James Broberg, and Andrzej M. Goscinski, eds. *Cloud computing: Principles and paradigms.* Volume 87, 2010.

[4]. SrijitaBasu, ArjunBardhan et. al. "Cloud Computing Security Challenges & Solutions-ASurvey." *Annual computing and communication workshop and conference (CCWC),* February 2018 .

[5]. Manju Sharma , SadiaHussain and Shazia Ali "Cloud Computing Risks And Recommendations For Security". *International Journal of Latest Research in Science and Technology (IJLRT),* Volume 6, January-February 2017.

[6]. Vishakha M. Shelke , John Kenny "Data Security in cloud computing using Hierarchical CP-ABE scheme with scalability and flexibility" *International Conference on Smart City and Emerging Technology (ICSCET),* November 2018.

[7]. Navia Jose, Clara Kanmani A " Data Security Model Enhancement In Cloud Environment." *IOSR Journal of Computer Engineering (IOSR-JCE),* Volume 10, Mar. - Apr. 2013

[8]. Vishwanath S Mahalle, Aniket K Shahade " Enhancing the Data Security in Cloud byImplementing Hybrid (RSA&AES) Encryption Algorithm." *International Conference on power, Automation and Communication (INPAC) ,* October 2014

[9]. MahalakshmiJeyabalu_y, KuppusamyKrishnamoorthy " Hybridization of ICBC and Genetic Algorithm for Optimizing Encryption Process in Cloud Computing Application Service." *Fundamental Informaticae*, Vol. 157, January 2018

[10]. Purnima Gupta, Deepak kumarverma, Aswani Kumar Singh" Improving RSA algorithm using multi-threading model for outsourced data security in cloud storage" *International Conference on Cloud Computing, Data Science & Engineering (Confluence)* , August 2018

[11]. HimelDey, RifatAslam, HossainArif "An Integrated Model To Make Cloud Authentication And Multi-Tenancy More Secure " *International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST),* February 2019

[12]. S. Bhute and S. K. Arjaria, "An efficient AES and RC6 based cloud-user data security with attack detection mechanism," Volume 3, 2016.

[13]. K. H. Patel and S. S. Patel, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" Volume 4, 2016

[14]. A. P. S and K. Subhashri, "Securing Outsourced Data On Cloud Using ElGamal Cryptosystem", 2017.

[15]. S. K. Majhi, "An Authentication Framework for Securing Virtual Machine Migration". *Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI),* September 21, 2016

[16]. FenghuaZhang,YamingChen,WeimingMeng and Qingtao Wu, "Hybrid Encryption Algorithms For Medical Data Storage Security In Cloud Database". *International Journal of Database Management Systems (IJDMS),* Volume 11, February 2019.

[17]. SumanMadana, PuneetGoswami, "A novel technique for privacy preservation using K-anonymization and nature inspired optimization algorithms". *International Conference on Sustainable Computing in Science, Technology & Management (SUSCOM),* 2019

Author'sBiography

Ms. Priyanka Singh received her Bachelor's degree (B.Tech) in Information Technology from GGSIPU, New Delhi, India. She is pursuing her Master's (M.Tech) in Information Security from AIACTR affiliated with GGSIPU, New Delhi, India. Her primary research area is in Network Security, Data Security, and Cloud Computing. She has communicated survey and research papers in conferences.

Dr. Manju Khari an Assistant Professor in AIACTR, Under Govt. Of NCT Delhi affiliated with GGSIP University, Delhi, India. She is also the Professor- In-charge of the IT Services of the Institute and has experience of more than twelve years in Network Planning & Management. She holds a Ph.D. in Computer Science & Engineering from National Institute of Technology Patna and She received her master's degree in Information Security from AIACTR, formally this institute is known as Ambedkar Institute of Technology affiliated GGSIP University, Delhi, India. Her research interests are software testing, software quality, software metrics, information security and nature-inspired algorithm.

How to Cite

Singh, Priyanka, and Khari,Manju(2019). A Survey of Cloud Computing Security Issues. *International Journal of Machine Learning and Networked Collaborative Engineering*, 3(04) pp182-192.

doi : https://doi.org/10.30991/IJMLNCE.2019v03i04.001