Brainwave: A Multidisciplinary Journal (ISSN: 2582-659X), Vol. 2, Special Issue No. 1, May 2021, pp. 60-69,


# A Review on Information Security in Cloud Based System during Covid-19 Pandemic

**Paramita Chatterjee[*#], Shantanu Mukherjee[#], Rajesh Bose[#], Sandip Roy[#]**
[#] *Department of Computational Science, Brainware University, India*
**pc11april@gmail.com*

**Corresponding Author*

## Abstract

*Work from Home is the new trend in corporate working culture in this Covid-19 pandemic situation. Of course it is a preventative measure to avoid the infection from the disease. Not only companies or corporate world but also education sectors are hugely depending on "online study" as schools and colleges are closed during the pandemic period. Cloud computing is the way that employees and students/teachers can work from home by using this. While using this cloud computing environment, users are using their own private network to accomplish the work and hence the security and privacy factor is major challenges to its user as this paradigm shift is involved with data protection, network security, virtualization security, application security etc. To prevent these security measures lots of researches going on. In this paper authors have tried to take some preventive solution, by going through different research paper and journals, analyzing the risk factor issues and minimize the risk factor. The objective is to underline the principal risk factors in cloud environment and find out the technical solution to it from log in, using the cloud to log out.*

*Keywords: information security, cloud security, pandemic threat, authentication, confidentiality, access control, integrity, cloud database.*

## I. Introduction

Currently the new working pattern in corporate and educational sector, which is work from home or online study, wholly depending on cloud computing. During the pandemic situation, to avoid the infection users are trying to fulfill their individual work from any places using private network. Same way students or teachers are continuing their academics from their own places which are geographically different. All are using or connected a common platform through cloud computing. This whole cloud based system gives its user to access a huge and variety of database via internet. Now where every moment users are dealing with huge data, obviously there comes a data storage centre and its subsequent management system [2]. The total infrastructure consists of storage device, software, hardware interfaces and communication network. This whole cloud service model involves three types of participants. Those are Service provider, Programmers and end users. Service providers are maintaining and monitoring the service i.e. the infrastructural parts are taken care by them. Programmers are responsible for delivering the services from the infrastructure to end users. The end users are using the whole features of cloud service through internet to accomplish their individual and corporate tasks from different geographical positions [1]. Now as multiple users, whether it is corporate employees or students and teachers, are sharing the same platform in cloud service, there comes the main concern which is security challenges. As the cloud computing system depending on some technicalities, there are different security level protocols like Saas, PaaS, IaaS, which is managing the security system effectively. When we are mentioning security concerns, we are keeping in mind Data lost, Data Protection, Data theft, data malfunctioning, Data share

etc [3]. In this paper we are trying to describe the common security issues faced by users and the possible solution to minimize the risk factors by analyzing the different related journals and researches. The following pandemic threats are generally recommended for measures in work from home culture or online study culture as in both cases private or public network uses for accessing huge data from multiple source which stored by multiple service provider.

| **Threats and other issues associated with Online Education/Work from home culture [16]** | | | | |
|---|---|---|---|---|
| **Data Privacy** | **Internet** | **Application** | **Personal Devices** | **CCE** |
| ✓ Malfunctioning<br>✓ Loss<br>✓ Copying<br>✓ Quality<br>✓ Availability | ✓ Availability<br>✓ Traffic<br>✓ Service | ✓ Technology Infrastructure<br>✓ Service | ✓ Infected old devices<br>✓ Malware<br>✓ Hacking | ✓ Data Storage<br>✓ IT Infrastructure<br>✓ Cost |

**Table I**

## II. Related Works

We have gone through related works and found that there are many research work going on Information Security and Cloud Security to minimize the risk factors by suggesting optimum measures. Viewpoints of few papers are as given below:

In [1] described Key aspects of cloud computing and its security and privacy. In [3] described the security problem in Cloud computing and resolve with quantitative security risk assessment model known as Multi-dimensional Mean Failure Cost ($M^2FC$).In paper [8] describes that the database security, privacy and its ethical issues. In paper [9] we can see the authentication security related to SSO, multi factors, username password, public key infrastructure etc. In paper [13] shows data security by digital signature with RSA algorithm. In paper [15] author discussed about malware threats and privacy protection, its detection process to resolve the privacy risk concern. The paper [16] explains the impact of Covid-19 pandemic situation on Cloud Computing. In paper [17] described about Fog Network its pre distribution, revealing the TD-R. In paper [19] discussed about Mobile Cloud computing and its security threats like malware behavior and its detection. In paper [20] we can see security transparency framework by incorporating an implementation process. In paper [21] describes about security risk assessment and systematically gain a distinction in multiple system resources and same security defense priority level. In paper [22] shows a comprehensive survey of intrusion detection systems that use computational intelligence in a mobile cloud environment. In paper [23] author proposes a secure data stream

outsourcing scheme with publicity verifiable integrity in cloud storage. In paper [24] author presented secure and effective scheme for storage of shared dynamic data in unstructured cloud server by integrity checking of third party service provider. In paper [25] introduces new technique of storing data in cloud network by file type classification. In paper [27] describes and proposed a new threshold hybrid encryption for integrity audit without trusting the data centre or data service provider.

## III. Information Security

Information security is a bunch of measures taken to keep the data secured from unauthorized access or alteration, in transmission or transition from one to another location as well as when it is getting stored. Sharing information is like sharing knowledge and knowledge is a most valuable asset one can have. The basic aspects or motto of information security are

- ✓ Availability
- ✓ Integrity
- ✓ Confidentiality

The main intension of Information security is to give its user confidence that they can share their thoughts or knowledge with having fear of any unwanted malpractice. It is protecting an organization from unwanted interference in confidential business information from its beginning. In educational sector it is so important to have right kind of information as per user need to get oneself updated about a particular subject whether it is for student or teacher.

Now when users start using the cloud system, first thing should taken care of is confidentiality so that it get encrypted, next thing should keep in mind that integrity so that the encrypted data remain same as it was created, third thing should keep in mind that availability of data as an when it needed.

In information Security there are different categories that shown in Figure 1.

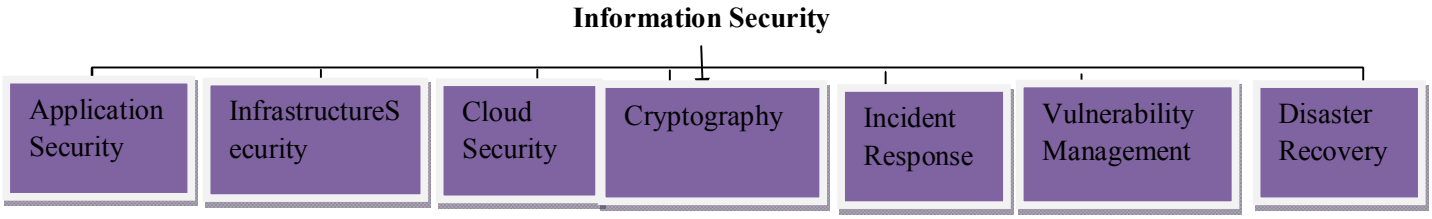


**Fig 1 [14]**

Also following figure 2 is showing various risk or threats associated with information security that should respond immediately to minimize the impact of unauthorized and unexpected outcome.

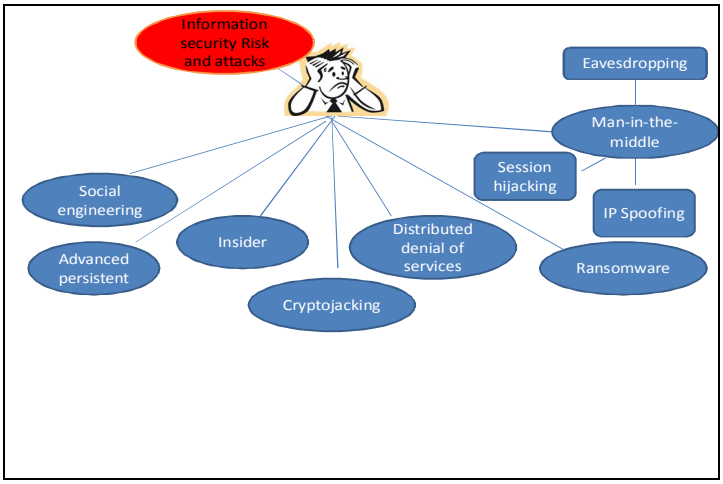


**Fig.2**

To prevent the above risks there are various security measure technologies applied in information security industry. They are

- Firewalls
- Security incidents and event management
- Data loss prevention
- Intrusion detection system
- Intrusion prevention system
- User behavior analytic
- Blockchain Cybersecurity
- Endpoint detection and response
- Cloud security posture management

## IV. Cloud Computing-Security Aspect

Security is one of the biggest concerns among the users as there is involvement of internet technology. The reason behind is internet is having loophole that can create insecurity by hacking, crashing, accessing the unauthorized details and there are specialized hackers available in worldwide. It is tuff to provide exact solution to it but we can minimize the risk factors by

- ✓ Providing entry level authentication security,
- ✓ Carefully handled encrypted data,
- ✓ Managing and storing massive amount of data.
- ✓ Secure control over accessing the data.

As we have already mentioned about different level of security protocols in cloud system model, the following figure 2 is describing the different cloud level services structure in cloud system [5].

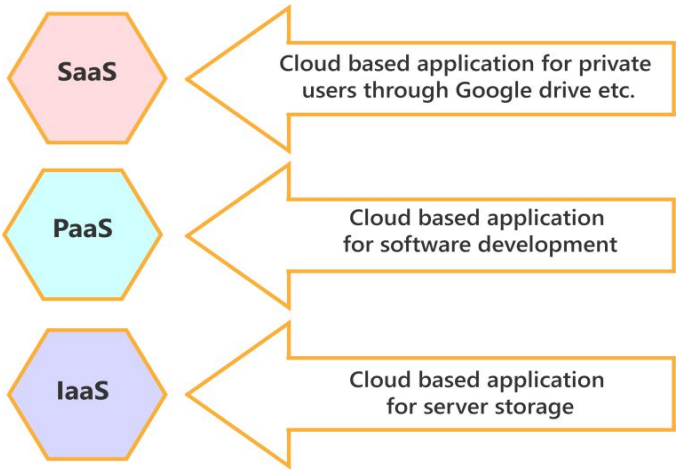


**Fig.3 Cloud: Level of Service [5]**

The following table II is describing different security attacks in cloud system delivery structure [5]

| Software as a Service (SaaS) | Platform as a Service (PaaS) | Infrastructure as a Service (IaaS) |
|---|---|---|
| Data Security | Data Location | Web Service Attack |
| Network Security | Privileged Access | SLA attack |
| Data Integrity | | DDoS Attack |
| Data Segregation | | MITM Attack |
| Data Breaches | | DNS Attack |

**Table II**

**SaaS level security**: Service provider has to measure security as huge level of date need to handle from different source. Users have to depend on the service provider as they are little confused about their security. The types of risk are mentioned in above table II.

**PaaS level security**: In this level of security users faces risk at different software platform and access.

**IaaS level security**: In this level user faces mainly data storage related security. The different type of security attacks in this level shown in the table II.

The following table III will describe the different implementation model in cloud system [6], [7].From this also we can assess the risk involved in each model.

| Public Cloud | Private Cloud | Community Cloud | Hybrid Cloud |
|---|---|---|---|
| Users can use this cloud through internet which is accessible for mass users. | Users are restricted as per as accessibility is concern, mainly used by inter organizational communication or information.. | It is mainly managed by more than one organization for particular secured communication or exchange of information. Mixture of Private, Public and Hybrid model. | Combination of Private, Public and Community cloud mostly controlled by third party service provider. |

**Table III**

The whole cloud system is the medium of exchanging or sharing information or sharing communication in current technological era. And internet is the technology of the cloud system thorough which this information shared by the end users.

**A. Authentication**: In cloud system, cloud is used to store data of users in a definite location which is maintained by different service provider or third party [9]. Every time user need to properly access to the said data through internet network. To have a proper access, authentication is the step to ensure the exact login entity so that user can have secure access to his needed data [8].

The cloud authentication is having multiple natures as [9]:

- Trusted Computing group
- Single sign on(SSO)
- Public key infrastructure
- Multi factor
- Username and Password
- Biometric
    1. Physical biometrics
    2. Behavioral biometrics

Some Techniques of Authentication [9]:

a. Data Access and Secure Storage (hidden policy method)
b. Access Control (Semantic-based) for needful security of Data
c. To improve Data access security using encryption ( location-based)
d. Based on Data classification secure model of cloud computing
e. Scalable authentication (User)
f. Digital Signature Authorization and Geo Detection
g. For private access approach of Trust management
h. Mechanism of 1-,2-,and 3- factor authentication

**B. Integration**: Cloud Integration is a process of different technologies combines various applications, systems, and other IT environments for sharing and storing data. After assembling these all the data and integrated cloud service is ready to use by users from multiple devices through internet [10]. Two types of integration is there they are Data Integration and Application Integration.

**C. Confidentiality**: This is an major part of security measure for user's data protection in the cloud. It sees whether the data been exactly encrypted and received without distortion. For example DELL provide hardware and software based encryption as well as transparent file encryption [8, 11].

**D. Access control and Authorization**: Access control and authorization is one of the key security measures so that the original and authentic user can access the data from cloud. It gives proper specification or recognition to the users at the time of log in to network or internet to get the needed data from cloud. The example of access control is McAfee which act as vendor to the cloud control and Oracle Vault is technique by which apply authorization [8].

**E. Database Security**: Database Security enables the security measures to stored database in the cloud in respect of malfunctioning, theft of data, loss of data during transaction and ethical practice on data use. There are following types of data security against which we should take mitigation approach [7]:

- Insecure Application Programming Interface (API)
- Malicious Insider
- Data loss
- Atrocious use of cloud computing
- Account and Traffic Hijacking
- Shared technology unprotected
- Unknown risk profile

**F. Encryption**: Data encryption is a process to transform a data to a another form or code and only authorized users can access with private key or password [12].

**G. Digital Signature**: It is a mathematical Approach towards authentication of data user so that the other end believes that it has send by actual author [13].

**H. Internet of Thing (IoT)**: It is a combined process of interconnected physical object that connected through internet to exchange data on wireless network. The example is Home security services, Biometric etc [10].

**I. Mobile network or Fog Network in Cloud computing**: The fog network or mobile network or multi network is a distributed network which is connected through a hardware device with remote service provider. It is a specific area oriented network. The example is network through router [17, 18].
The following figure 4 is showing Fog Network

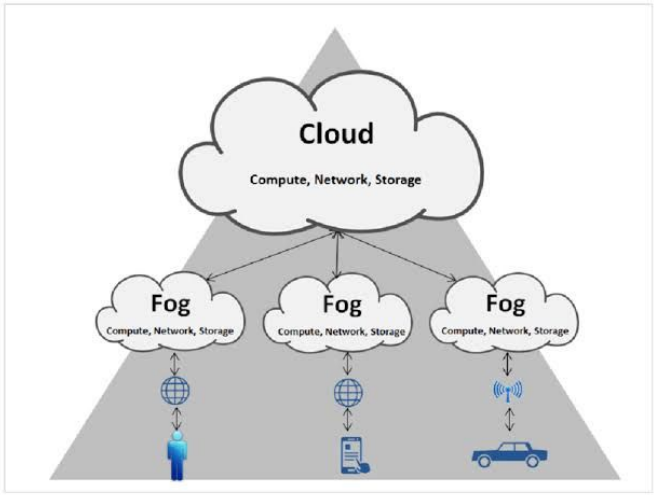


**Fig 4 Fog Network or Mobile Network [18]**

In commercial or organizational level there are many service providers providing services at different level of cloud security [14, 15]. Some of are as follows

- ✓ Amazon Web Services (AWS) providing remote access to cloud service with data protection
- ✓ Amazon EC2 is providing tailor made multilevel security
- ✓ Microsoft Windows Azure is protecting confidentiality of user in cloud data access.

## V. Cloud Computing Security during Pandemic-Conclusion

Novel corona virus is the reason for current pandemic situation in almost more than 120 nations all over the world. People of the world hugely effected as Govt. declared lockdown to stop spreading the infection. All the companies and corporate world adapted new working culture that is work from home. Not only corporate world affected but also it got huge impact on educational sector too. Educational sectors are also stated online classes or e learning to continue their course of studies [16]. Cloud Computing (CC) platform is only way to accomplish the individual work done. With the increasing trend of using CC the related technology is becoming complex to handle huge data source. And hence the security risk is getting higher day by day which we have to minimize by proper detecting and providing optimum solution in near future.

## References

[1] Pedro Ramos Brandao , *"Cloud Computing Security"* ,International Journal of Computer Science And Technology(IJCST). Vol.10, Issue 1,pp 26-32.ISSN: 0976-8491.March 2020.

[2] Lynda Kacha , Abdelhafid Zitouni , *" An Overview on Data Security in Cloud Computing"* ,Advances in Intelligent Systems and Computing 661,pp 250-260.DOI: 10.1007/978-3-319-67618-0_23.Springer, September 2018.

[3] Mouna Jouini , Latifa Ben Arfa Rabai , *" A Security Framework for Secure Cloud Computing Environments "* ,International Journal of Cloud Applications and Computing . Vol.6,Issue 3,pp 32-42.July 2016.

[4] https://www.exbeam.com/information-security. Accessed on February 2021

[5] Manahel Omar Hussen , Nirmala Sharma , Hosam F.El-Sofany , Fakhry Abbas, *"A Novel Model For Securing Access of Cloud-Based E-Learning Systems"* ,International Journal of Engineering Applied Sciences and Technology. Vol.4,Issue 7,pp1-9.ISSN No.2455-2143. December 2019.

[6] Paramita Chatterjee, Rajesh Bose ,Sandip Roy , *" A Review on Architecture of Secured Cloud Based Learning Management System "*,Journal of Xidian University .Vol.14, Issue 7,pp 365-376. ISSN: 1001-2400.July 2020.

[7] A.A.Izang , A.O.Adebayo ,O.J. Okoro , O.O.Taiwo , *" Security and Ethical Issues To Cloud Database"* , The Journal of Computer Science And ITS Applications . Vol.24, No. 2,pp 65-75.December 2017.

[8] Kire Jakimoski ,*"Security Techniques for Data Protection in Cloud Computing",* International Journal of Grid and Distributed Computing .Vol.9, No.1(2016).pp 49-56. ISSN: 2005-4262. 2016.

[9] Seyed Milad Dejamfar ,Sara Najafzadeh , *" Authentication Techniques in Cloud Computing :A Review"*, International Journal of Advanced Research in Computer Science and Software Engineering. Vol.7, Issue1, pp 95-99.ISSN: 2277128X. January 2017.

[10] Alessio Botta, Walter de Donato , Valerio Persico, Antonio Pescape, *" Integration of cloud computing and Internet of Things: A Survey",* Future Generation Computer Systems (2015),http://dx.doi.org/10.1016/j.future.2015.09.021

[11] Rajesh Bose, Debabrata Sarddar ,"*A Secure Hypervisor-based Technology Create a Secure Cloud Environment"*, International Journal of Emerging Research in Management & Technology. Vol.4,Issue 2,pp 44-49.ISSN:2278-9359.February 2015.

[12] Jinan Shen, Xuejian Deng ,Zhenwu Xu *,"Multi-security-level cloud storage system based on improved proxy re-encryption"*, EURASIP Journal on Wireless Communications and Networking 2019:277,pp 1-12.https://doi.org/10.1186/s 13638-019-1614-y.Springer,2019.

[13] Vrunda Gor, Gayatri Pandi (Jain), "*Enhancing Data Security using Digital Signature in Cloud Computing*", International Research Journal of Engineering and Technology (IRJET) .Vol.06, Issue 12,pp 1071-1076.ISSN 2395-0056.December 2019

[14] Ali Gholami , Erwin Laure ," *Security And Privacy of Sensitive Data In Cloud Computing: A Survey of Recent Developments"*. Computer Science & Information Technology(CS & IT).pp 131-150.DOI: 10.5121/csit.2015.51611.CSEIT,SPM-2015.

[15] Xianwei Gao, Changzhen Hu, Chun Shan ,Baoxu Liu,Zequn Niu, Hue Xie *,"Malware classification for the cloud via semi-supervised transfer learning"* ,Journal of Information Security and Applications.Vol.55,2020,102661,ISSN 2214-2126.Elsevier.December 2020 .

[16] Ziyad R.Alashhab, Mohammed Anber,Manmeet Mahinderjit Singh ,Yu-Beng Leau,Zaher Ali Al-Sai,Sami Abu Alhayja'a, *"Impact of coronavirus pandemic crisis on technologies and cloud computing applications",*Journal of Electronic Science and Technology.100059.ISSN: 1674-862X.Elsevier.November 2020.

[17] Nafiseh Masaeli, Hamid Haj Seyyed Javadi, Sayed Hossein Erfani, *"Key pre-distribution scheme based on transversal design in large mobile fog networks with multi-clouds*", Journal of Information Security and Applications.Vol.54,102519. ISSN 2214-2126. Elsevier. October 2020.

[18]https://hindujab.medium.com/the-architecture-of-fog-network-a-bridge-between-cloud-and-iot-part-2-a45612145a0b. Accessed on February 2021.

[19] Jannath Nisha O.S, Mary Saira Bhanu S, *"Detection of malicious Android applications using Ontology-based intelligent model in mobile cloud environment"*, Journal of Information Security and Applications. Vol.58, 102751, ISSN: 2214-2126. Elsevier.2021.

[20] Umar Mukhtar Ismail, Shreeful Islam, "*A unified framework for cloud security transparency and audit"* ,Journal of Information Security and Applications. Vol. 54,102594,ISSN: 2214-2126. Elsevier.October 2020.

[21] Amartya Sen, Sanjay Madria, *"Application design phase risk assessment framework using cloud securitydomains"*, Journal of Information Security and Appications . Vol.55,102617.ISSN:2214-2126. Elsevier. December 2020.

[22] Shahab Shamshirband, Mahdis Fathi, Anthony T.Chronopoulos, Antonio Montieri, Fabio Palumbo, Antonio Pescape, *"Computational intelligence intrusion detection techniques in mobile cloud computing environments:*

*review,taxonomy,and open research issues*" , Journal of Information Security and Applications.Vol.55.102582.ISSN:2214-2126.Elsevier. December 2020.

[23] Qiyu Wu, Fucai Zhou, Jian Xu, Qiang Wang, "*Secure data stream outsourcing with publicly verifiable integrity in cloud storage*",Journal of Information Security and Applications. Vol. 49,102392.ISSN: 2214-2126. Elsevier. December 2019.

[24] Surmila Thokchom, Dilip Kr.Saikia, "*Privacy preserving integrity checking of shared dynamic cloud data with user revocation*", Journal of Information Security and Applications. Vol. 50,102427. ISSN:2214-2126. Elsevier. February 2020.

[25] Sahana ,S., Bose,R. & Sarddar, D., "*Harnessing RAID mechanism for enhancement of data storage and security on cloud*", Braz J Sci Technol 3,12(2016).

[26] Shynu P.G., Nadesh R.K., Varun G.Menon, Venu P., Mahdi Abbasi,Mohammed R.khosravi, "*A secure data deduplication system for integrated cloud –edge networks"*.Journal of Cloud Computing :Advances,Systems and applications.9:61.https://doi.org/10.1186/s13677-020-00214-6.Springer. 2020.

[27] Yange Chen ,Hequn Liu, Baocang Wang, Baljinnyam Sonompil,Yuan Ping, Zhili Zhang , "*A threshold hybrid encryption method for integrity audit without trusted center"*, Journal of Cloud computing : Advances,Systems and Applications.10:3.https://doi.org/10.1186/s13677-020-00222-6.Springer.2021