# Data Security Issues and Solutions in Cloud Computing

**Malith M.C. Ranasinghe**
Sri Lanka Institute of Information Technology (SLIIT)
Faculty of Computing, Department of Software Engineering

Student ID : IT18097634

***Abstract*** **-**Cloud computing is a model of managing, storing, processing data online via the internet. This creates a world where everyone is connected to access specific data regardless of where the location . Though cloud computing allows numerous benefits for organizations as well as personals this includes many security issues. Therefore there is a tendency of feeling of fear to store data in cloud computing. However it's a trust between users and service providers. This paper includes an analysis related to security issues in cloud computing data , and provided solutions.

*Keywords:* cloud, delivery model, encryption, security, SAAS,PAAS,IAAS

## 1. INTRODUCTION

Cloud computing is a type Internet based computing which provides you shared processing resources and data to systems and other devices on respective demand [1]. It's a model of managing, storing, processing data online via the internet. Without owning or maintaining data centers and servers physicallycloud computing enables access servicesfrom a cloud provider like Amazon Web Services. Organizations are using the cloud for a wide variety of purposes, such as data backup, email, software development and testing, disaster recovery, virtual desktops, big data analytics, and customer facing web applications. With cloud computing business can align with agile, reduce costs, improve mobilization,saves time, go green, independency of devices and location, and has security due to centralization of data [1]. Data storage can be identified as one of the main services provided through cloud computing. Cloud service provider hosts the data of data owner on their server and user can access their data from these servers.Therefore, security and privacy has become a key issue in cloud computing [2]. To serve the users better cloud services needs to incorporate high security methods. In order to implement security first it is crucial to identify the security issues that encounter in cloud computing. Once the issues are identified it is easy to implement methods to protect the data from the threats.

## 2. DISCUSSION

### Cloud Computing Backgroud:

There are 3 delivery modules identified in cloud computing [3].

**SAAS(Software As a Service):** This is a service that offers On-Demand Service, which is Pay Per Use of Application Software to Users. It's independent platform which does not need to Install The Soft wear On the PC. Examples for SAAS are, Gmail, ,Google Drive, Google Docs.
**PaaS or platform-as-a-service:** Thisis mainly based on development environment .Examples as Windows Azure,Google App Engine ,Heroku and force.com
**laaS or infrastructure-as-a-service:** this service offers all computing resources but in a virtual environment so that multiple users can access them. These resources include servers ,data storage,virtualization,and networking.
When considering the types of cloud computing there are 5 types [4].

1)Public Cloud: Service available for the general public or industry group. (Eg: Microsoft, Amazon AWS).Same infrastructure shared by all the users.

2)Private Cloud:Service available only for a specific organization.
3)Community Cloud: The service available for several organizations that work for common goals.
4)Hybrid Cloud: This is a combination of two or more clouds.
5)Federated Cloud: It's combination of smaller services.
When comparing all above types public cloud seems encounter more security issues than others.

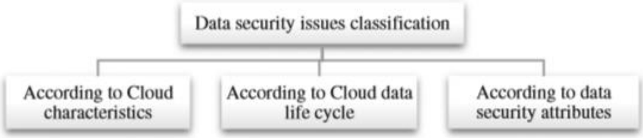
In order to have a proper well-functioning cloud computing facility there are some key principles which needs to fulfill.
**Confidentiality** : Cloud computing storage belongs to third parties. Therefore the confidence between the vendor and the customer needs to be there always that the data can be accessed by the authorized partied only and the data is restricted for others. There is always the risk of Insider user threats as well as external user threats. If by any chance due to an error there is possibility of data leakages which will affect confidentiality directly.
**Integrity:** This refers to maintaining accuracy of data avoiding any modification to data by unauthorized parties. Due to attacks if the segregation of data is not properly maintained there might be issues. At the same time users may lose the connection to access data. Further if the data is manipulated the quality of data gets harmed. Therefore integrity is one of the key principles that should look into in data security.
**Availability:** The data should be available at any time for the authorized parties to access based on the demand. Network issues, hardware issue, system crash possible in cloud computing and the solution is to have data backup for such circumstances.

## Security Issues:

Top seven security issues in cloud computing environment as discovered by "Cloud Security Alliance" CSA are [5]:

- Misuse and reprehensible use of Cloud Computing.
- Insecure API.
- Wicked Insiders.
- Shared Technology issues / multi-tenancy nature.
- Data Crash.
- Account, Service & Traffic Hijacking.
- Unidentified risk report.

There are many risks and security issues involved with cloud computing and its data. Xiaotong Sun in the survey [6] has highlighted 3 dimensions of cloud computing security as computer security, Network security, and information security. Information security is based on 3 principles of Availability, IntegrityandConfidentiality [7].
Information Security has issues in different areas as Losing control over data, Data integrity, Risk of Seizure, Incompatibly issues, Constant feature additions, Failure in Provider's security, Cloud provider goes down [7].
Although there are different types of classification of data security in cloud computing Lynda Kacha(&) and AbdelhafidZitouni has chosen the blow categorization in their explanation [8].


Data security issues classification
According to Cloud characteristics
According to Cloud data life cycle
According to data security attributes

Data Security Issues Classification [8]

The security issues identified according to cloud characteristics are leased infrastructure, open infrastructure, shared infrastructure, Elastic infrastructure, Virtualized infrastructure, Distributed infrastructure. It is obvious that these characteristics have an impact on data security. There are 3 states related to the data in cloud. Those are data at rest(Data Storage), data in-transit, and data in use. One of the main services from cloud computing is data storage. The storage for cloud computing gives the customer unlimited space. Security in storage media in critical such as

risks associated with shared storage media, Risks related to data location, and also the risks relevant to reliability of the data storage [8]. Users does not have control over the stored data in data centers. The providers have the full control for modifications. The lack of control by users, concepts of multi–tenancy and virtualization have high security risks associated with Cloud computing than information stored in traditional data center [9].
While data transmission there is a possibility that the data can be modified. During the processing time the data is not encrypted. In homomorphism encryption which allows the data to be processed without being decrypted [5].

## Data Security Solutions

Data protection at the storage could be the combined efforts taken by both cloud provider and user by maintaining privacy and integrity [9]. User and the service provider both have equal responsibilities in order to protect data in cloud computing. The contribution from the storage media is also considerable. The weighted sum of below parameters are considered to be equal for the data protection(D1) in the analysis done by Rizwana A.R. Shaikh and Masooda M. Modak [9].
Encryption from user side(EN1): Depending on the key size the user chooses that is assumed that the 30% of strengthen is achieved.

Encryption from server side(EN2):30% strength.

Disk leakage property(DLM): This is referred to the media used to store data in cloud computing. Compact disk, magnetic disk are more suitable for storage media and the assumption is that 20% of the storage protection comes from the above.

Integrity strength(INT):
D1= Sum (0.3(En1), 0.3(En2), 0.2(DLP), 0.2(INT))

Further to the above Update/Delete Anomalies, Transient data protection, back up and Disaster recovery plans are some of the other security solutions.
According to Lalitha V.P and Sagar M.Y, Sharanappa S, Shredar Hanji, Swarup R, it is proposed to encrypt and store data in cloud so that the user can modify data anytime. When assessing the performance analysis and data security, it clearly depicts that this increases work efficiency and also evade unauthorized users to access the data [10].

Bih-Hwang Lee and Ervin KusumaDewi, Muhammad FaridWajdi have proposed an execution for the data security in cloud computing using AES under Heroku cloud. There are several steps in implementation for deploying Heroku as a cloud platform. A website has also been implemented as an application of the data security and AES is impletemented as data security algorithm. As shown in the performance evaluation, AES cryptography is used for data security. Furthermore, the fact that larger size of data causes to increase the data delay time for encrypting data is shown in delay calculation of data encryption [11].

Hybrid Cryptographic System (HCS) has been proposed by Akshay Arora and Abhirup Khanna which is a combination of the advantages of both symmetric and asymmetric encryption. It ensures the data privacy and security by applying several encryption techniques at different levels. This uses some hashing and salting techniques which also result in strengthening the whole encryption process. Having the feature of One Time Password (OTP) helps in trusted authentication as well [12].

## 3. CRITIQUE

Based on the analysis on several research papers related to security in cloud computing and solutions I could confirm the below key points .

Cloud computing covers a vast area which includes data, network and all infrastructure. Cloud computing architecture itself is more complex. Based on the complexity I could see a tendency of having different types of classification related to security issues.

However above all the security issues most of the research are more keen on “data security issues” related to cloud computing. Since data has become a crucial element nowadays it’s good to have different perspective arguments.

Most of the analysis have focused on data characteristics, data types , and data states to highlight data security issues related to cloud computing. However my argument is that data issues can arise not only from data but also from different aspects like infrastructure issues, network issues etc.

When considering the solutions proposed in order to solve security issues in data cloud computing, most of the solutions are related to encryption which can be considered one element of data security. In my point of view ensuring security on encryption cannot guarantee the whole data security in cloud computing since other than encryption there are several other key aspects that affect security.

Moreover, data in cloud computing is based on the trust between the service provider and the user. Encryption security measures can be taken by both the user and the service provider. However it is questionable that who owns the data in cloud computing. In my point data should only own by the user. However service provider too have the possibility to access the same data. Therefore there is a gap in consist between legal issues related to data security.

At the same time user has the same obligation as the service provider to protect his/her data. User needs to update the password time to time. He has to follow the correct rules when creating the password. Using strong passwords leads to better the security. It’s better if the research could focus on users aspect as well when considering the data security solutions.

At last but not least what so ever security measures taken to secure data in cloud computing, with the rapid new technology changes hackers are always updated with new actions. Therefore it is essential to update the security solutions accordingly.

## 4. CONCLUSION

This review has focused mainly on data security issues and proposed solutions to overcome some security issues. With the increasing demand in Information Technology, cloud computing plays a major role by opening up new opportunities for businesses and also for the people who are truly interested in the field of computer sciences. Cloud computing enhances the efficiency and the flexibility of the businesses in order to meet the expanding needs. On the whole, this is a way of providing a service using hardware and software through a network. The term of cloud computing is commonly used to refer to the availability of the data centers for many users over the Internet. It is becoming increasingly popular nowadays since it provides the software, infrastructure, and the platforms that are needed for the accomplishments in modern business landscape. Most importantly, it has become a very convenient shared pool for its users. In addition, the widespread usage of cloud computing results in creating greater demand for the talented professionals who are able to manage these networks properly.

However based on some circumstances reported recently it is questionable whether the data is really secure in cloud computing. It is true that cloud computing allows organizations, users a huge set of benefits. However still there is fear to move to cloud computing due to security issues. Therefore in order to attract big organizations, and more users it is a must to update security measures always with the rapid technology changes. Security solutions needs to be far ahead in technical perspective when compared to hackers actions.

# References

[1] P. N. K.-V. P. S. M. S. Prof. Syed Neha Samreen1, "Introduction to Cloud Computing," *International Research Journal of Engineering and Technology (IRJET),* vol. 05, 2018.

[2] M. S. E. A Venkatesh, "A Study of Data Storage Security Issues in Cloud Computing," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* vol. 3, no. 1, 2018.

[3] M. D. E.-C. E. Ahmed EL-Yahyaoui, "Data Privacy in Cloud Computing," in *4th International Conference on Computer and Technology Applications*, 2018.

[4] S. a. B. Rajat Soni, "Security and Privacy in Cloud Computing," in *Symposium on colossal Data Analysis and Design* .

[5] D. H. Adnaan Arbaaz Ahmed, "CLOUD COMPUTING: STUDY OF SECURITY ISSUES AND RESEARCH CHALLENGES," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) ,* vol. 7, no. 4, 2018.

[6] X. Sun, "Critical Security Issues in Cloud Computing: A Survey," in *4th IEEE International Conference on Big Data Security on Cloud*, 2018.

[7] D. G. Ashima Narang, "A Review on Different Security Issues and Challenges in Cloud Computing," in *International Conference on Computing, Power and Communication Technologies (GUCON)* , 2018.

[8] L. K. a. A. Zitouni, "An Overview on Data Security in Cloud Computing," in *Conference Paper in Advances in Intelligent Systems and Computing* , 2018.

[9] O. A. A. A. Isaac Odun-Ayo, "An Overview of Data Storage in Cloud Computing," in *2017 International Conference on Next Generation Computing and Information Systems*, 2017.

[10] M. M. M. C. Rizwana A.R. Shaikh, "Measuring Data Security for a Cloud Computing Service".

[11] S. M. S. S. S. H. S. R. Lalitha V.P, "Data Security in Cloud," in *International Conference on Energy, Communication, Data Analytics and Soft Computing* , 2017.

[12] E. K. D. M. F. W. Bih-Hwang Lee, "Data Security in Cloud Computing Using AES Under HEROKU Cloud," in *The 27th Wireless and Optical Communications Conference* , 2018.

[13] A. K. ,. R. A. Akshay Arora, "Cloud Security Ecosystem for Data Security and Privacy".