DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5535

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

EFFICIENT DATA CONFIDENTIALITY AND PORTABILITY IN CLOUD STORAGE

Gagandeep Kaur
Department of Computer Engineering and Technology
Guru Nanak Dev University
Amritsar, India

***Abstract*:** In today's era, cloud computing becomes the hottest topic due to its ability to reduce the cost associated with computing. Cloud computing provides the on-demand services like storage, servers, resources etc. to the users without physically acquiring them and the payment is according to pay per use. Since cloud provides the storage, reduces the managing cost and time for an organization to the user but security and confidentiality become one of the biggest obstacles in front of us. The major problem with cloud environment is the number of the user is uploading their data on cloud storage so sometimes due to lack of security, there may be chances of loss of confidentiality. To overcome these obstacles a third party is required to prevent data, data encryption, and integrity and control unauthorized access to data storage to the cloud. Cloud portability becomes critical in the situation of loss of confidentiality. To optimize better results we will review some paper and find the better results to remove the security barriers.

KEYWORDS: Cloud Computing, security, confidentiality, portability

1. INTRODUCTION

With the rapid development of hardware and software cloud computing brings the revolution in the business industry[1]. It provides resources like computational power, storage, computation platform ad applications to user on demand through internet. Some of the cloud providers are Amazon, IBM, Google, Sales-force, Microsoft etc.Cloud computing features includedresource sharing, multi-tenancy, remote data storage etc. but it challenges the security system to secure, protect and process the data which is the property of the individual, enterprises and governments. Even though, there is no requirement of knowledge or expertise to control the infrastructure of clouds; it is abstract to the user. It is a service of an Internet with high scalability, quality of service, higher throughput and high computing power[2]. Cloud computing providers deploy common online business applications which are accessed from servers through web browser. Data security is the biggest issue in cloud computing and it is not easy to resolve it. In our review paper we will review the different ways to manage the confidentiality of the data[3].

2. OBJECTIVES

The main objectives of this research are given below:

- To comprehend the security issues and to recognize the suitable security systems those are being utilized as a part of the present universe of Cloud Computing.
- To recognize the security challenges those are normal later on of Cloud Computing[4].
- To propose some counter measures for the future difficulties to be looked in Cloud Computing.

3. OVERVIEW: SECURITY ISSUES IN CLOUD COMPUTING

In cloud environment usual data transmission occurs between client and server using the third party. So the confidentiality of your data becomes the primary problem. Security issues for a significant number of these frameworks and innovations are pertinent to distributed computing[5]. For instance, the system that interconnects the frameworks in a cloud must be secure and mapping the virtual machines to the physical machines must be completed safely. Information security includes encoding the information and additionally guaranteeing that suitable strategies are implemented for information sharing[6]. Cloud security isn't to be mistaken for "cloud-based" security benefit over the conventional danger. This security administration can be upgraded with the distributed computing, ensuring against DDOS, Trojan, Virus, and Spam and so on more viable than any other time in recent memory[7].

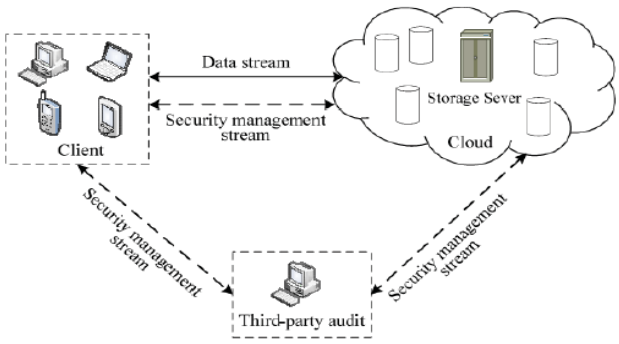

Figure 1: Data storage structure of Cloud Computing

However, the qualities of distributed storage make clients' information looked at numerous security dangers, incorporates: (1) the conventional security district parcel is

invalid. On account of the distributed storage benefit must be adaptable, security limits and assurance hardware can't be unmistakably characterized, which builds some trouble for the usage of particular assurance measures; [8](2) the distributed storage transmits information through the system. The benefit interferences, information devastation, data stolen furthermore, altered caused by the noxious assaults in the organize represent a serious test to the security of information correspondences, get to confirmation and classification; [9](3) from the client's view, the distributed storage of information makes distributed computing specialist co-op gets the information get to control, and the client's information is looked with protection security dangers. Individuals stress over that the touchy individual information will be exposure, abuse or missing by putting the information in cloud condition[10]. To tackle the above issues, as of late, scientists made a parcel of research work in the information security to control systems, information respectability, confirmation, ciphertext to recover and information encryption system of cloud figuring condition[11].

There are lots of security issues with cloud computing because of technologies utilization including networks, operating systems, databases, resource scheduling, virtualization, load balancing, transaction management, memory management and concurrency control.For example, the network should be secure on a cloud so that mapping the virtual machines to the physical machines has to be carried out securely[12]. Data security not only involves encrypting the data but also gives surety of appropriate policies.Cloud computing suffers from some various security concerns which are given below.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management
-

4. CLOUD SECURITY CHALLENGES

Some of the cloud security challenges that come in front of users are given below:

1. Authentication: The data on the internet is available to all the unauthorized users. Therefore the confidentiality of the data can be lost.
2. Access Control: To give access to only legalized users some control policies are used.Theseservices must be adjustable, well planned, and their allocation is overseeing conveniently[13].
3. Policy Integration: There are many cloud providers they use their own policies and approaches. Some of them are Amazon, Google who provides services to end users.
4. Service Management: In this different cloud providers such as Amazon, Google, comprise together to provide services to meet their customers need.
5. Trust Management: The trust management approach must be developed so that trust remains between both parties such as user and provider.

5. SECURITY FEATURE IN CLOUD COMPUTING

There are several main challenges for building assurance to the user:

1. Outsourcing: Outsourcing cuts down both capital consumption and operational use for cloud clients. In any case, outsourcing additionally implies that clients physically lose control of their data and undertakings. The loss of control issue has turned out to be one of the main drivers of cloud uncertainty [14]. To address outsourcing security issues, initially, the cloud supplier should be reliable by giving trust and secure computing and data stockpiling; second, outsourced data and computation might be evident to clients as far as classification, honesty, and other security administrations. Likewise, outsourcing will possibly bring about security violation, because of the way that delicate data is out of the proprietor's control[2].
2. Massive data and intense computation: Cloud computing is fit for handling mass data stockpiling and intense computing assignments. Thusly, customary security components may not do the trick because of terrible computation or correspondence overhead. For instance, to check the respectability of data that is remotely put away, it is unreasonable to hash the whole data set. To this end, new systems and conventions are normal[15].

Security Issues

The security of corporate data in the cloud is troublesome, as they give distinctive administrations like Network as an administration (NaaS), Platform as an administration (PaaS), Software as an administration (SaaS), Infrastructure as an administration (IaaS). Each administration has their particular security issues.

1. Data Security: Data Security brings up to a secrecy, trustworthiness, and accessibility. These are the significant issues for cloud merchants. Classification is characterized as a protection of data. Secrecy is intended to keep the delicate data from unapproved or wrong individuals[16]. In this stores the encryption key data from big business C, put away at scrambled configuration in big business D. That data must be secure from the workers of big business D. Uprightness is characterized as the rightness of data, there is no regular strategies exist for affirmed data trades. Accessibility is characterized as data is accessible on time.

2. Administrative Compliance: Customers are in the long run responsible when the security and climatic stage of their own data is taken by a specialist co-op.[17] Traditional specialist organizations more inclined to outsource overviews and security confirmation. Cloud computing suppliers reject to bear the examination as flagging so these clients can just make use of insignificant operations. 3. Data Locations: When clients utilize, they likely won't know precisely where their data will facilitate and which area it will put away in. Truth be told, they won't comprehend what nation it will be put away in. Specialist organizations should be asked whether they will achieve to putting away and modify data specifically discretion, and on the premise of their clients will they make a reasonable achievement to take after neighborhood protection necessity[18].

4. Special client access: Outside the asset data that is prepared contains an indigenous chance, as to convey administrations, keep away from the mortal, reliable and human asset oversee IT shops deals with the house programs.

5. Put stock in Issue: Trust is additionally a noteworthy issue in cloud computing. Trust can be in the middle of human to machine, machine to human, human to human, machine to human. Trust is rotating around confirmation and certainty. In cloud computing, client stores their data on cloud stockpiling in light of trust on a cloud. For instance, individuals utilize Gmail server, Yahoo server since they trust on supplier[19].

6. Data Recovery: It is characterized as the way toward reestablishing data that has been lost, degraded or hazard.

Security Solutions

In order to overcome challenges that comes in front of cloud security, some technical solutions relevant to cloud security should be considered. In our paper we review four typical aspects of technical solutions for which are given below in table.

Table 1: Cloud Security Solutions

Security solutions	Description
Continuation Mechanism	The security solution of servicemigration from non-cloud platform tocloud platform.
IDM	Simplified authentication managementfor cloud environment and end-to-end Trustable access technology.
Data security	Data transmission, data isolation, datawiping
virtualization security	Virtualization Machine Monitoring(VMM) security, Virtual Machine(VM) security, and virtualization Network security.

1. Continuation of service from the traditional platform to cloud platform- In this era, every person is shifting his business applications to the cloud. Even though it is a good technology but it brings some risks in front of them [20].

2. Identity and access management- Unauthorized access to the information on the cloud becomes a big issue because all the confidential data is on the internet so anybody can access or trap the network. So it must be required updating the traditional approach of identity mechanism in order to get the higher level of security. Identity federation, security assertion markup, biometric sensors are some of the ways to secure data from unauthorized access.

3. Data Security- Data security is the common issue in the cloud environment. In order to maintain the confidentiality of data, availability, and completeness some encryption techniques can also be applied. For more security data wiping is also necessary so that sensitive information can't be leaked out [21].

4. Virtualization Security- Virtualization guarantees the cost saving, ease of administration etc. Virtual environment includes access control, virtual machine monitor; virtual firewall which provides security to the user that data is secure on the system [22].

Cloud Portability

The ability to move from one place to another without any change is known as portability. The word cloud portability means to move applications and its associated data from one cloud provider to another with less disruption and minimal downtime[23], [24]. It also includes the transfer of data between public and private cloud environment.

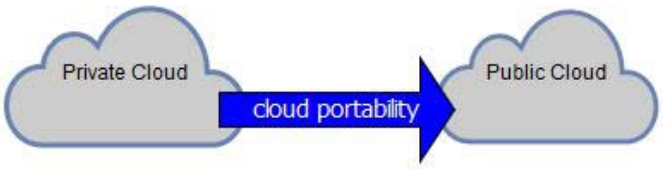

Figure 2: Cloud Portability

Today cloud computing is recognized as universal network access to shared and virtualized computing capability. Cloud portability can be majorly divided into three perspectives:

1. Implementation Perspective: This is related to portability which considers the specification and restriction on implementation. For E.g.: deployment descriptors, API calls.

2. Ecosystem Perspective: This portability considers the environment in which specific services are moved.
3. Business Perspective: This portability considers business related constraints like pricing, compliance etc.

The cloud portability also depending upon the software assets that are ported and can be categorized as follows:

Data Portability: It enables the clouds data component re-use and import – export functionality of data services.

Functional Portability: In this cloud services can transfer applications.

Service portability or platform portability is the ability to add, reconfigure and remove Cloud resources on the fly, independent on the Cloud provider.

6. COMPARISON TABLE FOR SECURITY TECHNIQUES

Comparison of distinct techniques showing enhancement parameters, focused area and techniques associatedwith the analyzed research. This table can be used to conclude future enhancement in existing techniques to improve security in cloud computing.

Table 1: Comparison table for security techniques used within cloud

Solution	Focused Area	Security Mechanism	Key Used	Enabled Sharing	Support Portability
Transparency [25]	Audit Facility for data validation	Audit facility	--	Yes	No
Symmetric Encryption[26]	Key based encryption for file required to be transmitted	Keys Based mechanism	Private key	Yes	Yes
Trust Mechanism [27]	Evidence, Validation, certification of attributes are critically analyzed	Evidence matching at source and destination end	--	Yes	No
Meta map reduce Computational Security [28]	Computational Security	Number of nodes as increases, computational complexity and threat increases. using Meta map reduce both metrics are reduced	--	Yes	No
Application partitioning [29]	Optimization of Cost in data transfer along with encoding mechanism for security concerns	Encoding and partitioning mechanism for placement of data n hybrid cloud	Public and private key based on cost optimization model	Yes	Yes
Channel Estimation Error[30]	Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors	Performance analysis of cloud is done by determining the security and reliability metric through channel estimation	-----	Yes	Yes
Access Control Mechanism[31]	On the Security of Data Access Control for Multiauthority Cloud Storage Systems	Access Control mechanism is used to ensure sharing of resources on the basis of access granted to user	Read/Write Permission	Yes	Yes
Order preserving encryption[32]	Security Analysis on One-to-Many Order Preserving	Packet order sequence is given priority and encryption suggest	Private key	Yes	Yes

	Encryption Based Cloud data Search	security enhancement mechanism			
Security and protection issues of cloud are discussed[33]	Data Security and Privacy Protection Issues in Cloud Computing	Survey of data security issues is being done	----	---	--

7. CONCLUSION AND FUTURE WORK

Cloud computing not only provides the resources to the users but also give a big challenge of security. There are securities requirements for both users and cloud providers but sometimes it may conflict in some way. Security of the cloud depends upon trusted computing and cryptography. In our review paper some issues related to data location, security, storage, availability and integrity. Establishing trust in the cloud security is the biggest requirement. These issues mentioned above will be the research hotspot of cloud computing. There is no doubt that cloud computing has bright future.

8. REFERENCES

[1] X. Yu, "Intelligent Urban Traffic Management System Based on Cloud Computing and Internet of Things," pp. 2169–2172, 2012.

[2] B. Mills, T. Znati, and R. Melhem, "Shadow Computing: An energy-aware fault tolerant computing model," *2014 Int. Conf. Comput. Netw. Commun.*, pp. 73–77, 2014.

[3] V. M. Sivagami, "Survey on Fault Tolerance Techniques in Cloud Computing Environment," no. 9, pp. 419–425, 2015.

[4] R. Jhawar, V. Piuri, and M. Santambrogio, "A Comprehensive Conceptual System-Level Approach to Fault Tolerance in Cloud Computing," pp. 0–4, 2012.

[5] C. A. Chen, M. Won, R. Stoleru, and G. G. Xie, "Energy-efficient fault-tolerant data storage and processing in mobile cloud," *IEEE Trans. Cloud Comput.*, vol. 3, no. 1, pp. 28–41, 2015.

[6] S. S. Lakshmi, "Fault Tolerance in Cloud Computing," vol. 04, no. 01, pp. 1285–1288, 2013.

[7] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," Proc. - 10th IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2008, pp. 5–13, 2008.

[8] Z. Xiao, W. Song, and Q. Chen, "Dynamic Resource Allocation Using Virtual Machines for Cloud Computing Environment," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1107–1117, Jun. 2013.

[9] U. Wajid, C. Cappiello, P. Plebani, B. Pernici, N. Mehandjiev, M. Vitali, M. Gienger, K. Kavoussanakis, D. Margery, D. G. Perez, and P. Sampaio, "On Achieving Energy Efficiency and Reducing CO 2 Footprint in Cloud Computing," vol. 7161, no. c, 2015.

[10] Y. Xie, H. Wen, B. Wu, Y. Jiang, and J. Meng, "Transactions on Cloud Computing," vol. 13, no. 9, 2015.

[11] D. Ardagna, G. Casale, M. Ciavotta, J. F. Pérez, and W. Wang, "Quality-of-service in cloud computing : modeling techniques and their applications," pp. 1–17, 2014.

[12] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, p. 50, 2010.

[13] S. Saha, S. Pal, and P. K. Pattnaik, "A Novel Scheduling Algorithm for Cloud Computing Environment," vol. 1, 2016.

[14] A. Farahzadi, P. Shams, J. Rezazadeh, and R. Farahbakhsh, "Middleware technologies for cloud of things-a survey ☆," *Digit. Commun. Networks*, no. April, pp. 1–13, 2017.

[15] J. P. D. Comput, B. Javadi, J. Abawajy, and R. Buyya, "Failure-aware resource provisioning for hybrid Cloud infrastructure," *J. Parallel Distrib. Comput.*, vol. 72, no. 10, pp. 1318–1331, 2012.

[16] J. Mohammed, C.-H. Lung, A. Ocneanu, A. Thakral, C. Jones, and A. Adler, "Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing," in *2014 IEEE International Conference on Internet of Things(iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*, 2014, pp. 256–263.

[17] X. Cui, B. Mills, T. Znati, and R. Melhem, "Shadow replication: An energy-aware, fault-tolerant computational model for green cloud computing," *Energies*, vol. 7, no. 8, pp. 5151–5176, 2014.

[18] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," *Globecom Work. (GC Wkshps), 2013 IEEE*, pp. 446–451, 2013.

[19] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," in *2010 IEEE 30th International Conference on Distributed Computing Systems*, 2010, pp. 253–262.

[20] H. Wang, Z. Kang, and L. Wang, "Performance-Aware Cloud Resource Allocation via Fitness-Enabled Auction," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 4, pp. 1160–1173, Apr. 2016.

[21] Z. Amin, "Review on Fault Tolerance Techniques in Cloud Computing," vol. 116, no. 18, pp. 11–17, 2015.

[22] P. Zhang, S. Hu, J. He, Y. Zhang, G. Huang, and J. Zhang, "Building cloud-based healthcare data mining services," *Proc. - 2016 IEEE Int. Conf. Serv. Comput. SCC 2016*, pp. 459–466, 2016.

[23] E. A. Alomari and M. M. Monowar, "Towards Data Confidentiality and Portability in Cloud Storage Towards Data Confidentiality and Portability," no. June 2014, 2016.

[24] P. You, Y. Peng, W. Liu, and S. Xue, "Security Issues and Solutions in Cloud Computing," 2012.

[25] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, and E. Dubois, "Security transparency : the next frontier for security research in the cloud," *J. Cloud Comput.*, 2015.

[26] S. Kaushik, "Cloud data security with hybrid symmetric encryption," pp. 0–4, 2016.

[27] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," pp. 1–14, 2013.

[28] P. Derbeko, S. Dolev, E. Gudes, and S. Sharma, "ScienceDirect Security and privacy aspects in

MapReduce on clouds: A survey," *Comput. Sci. Rev.*, pp. 1–28, 2016.

[29] N. M. Dhanya and G. Kousalya, "Adaptive and Secure Application Partitioning for Of fl oading in Mobile Cloud Computing," vol. 1, pp. 45–53, 2015.

[30] J. I. A. You, Z. Zhong, G. Wang, B. O. Ai, and S. Member, "Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors," vol. 2, 2014.

[31] X. Wu, R. Jiang, and B. Bhargava, "On the Security of Data Access Control for Multiauthority Cloud Storage Systems," pp. 1–14, 2015.

[32] K. Li, W. Zhang, C. Yang, and N. Yu, "Security Analysis on One-to-Many Order Preserving Encryption Based Cloud data Search," vol. 6013, no. c, pp. 1–9, 2015.

[33] D. Chen, "Data Security and Privacy Protection Issues in Cloud Computing," no. 973, pp. 647–651, 2012.

[34] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, 0Sep. 2013.

[35] V.Spoorthy and M.Mamatha," A Survey on Data Storage and Security in Cloud Computing", 2014.