

ANALYSIS ON SECURED EFFICIENT AND EXAGGERATED SECURITY FOR DATA SHARING IN MULTI- CLOUD STORAGE

Pruthviraj R. Pawar¹; Dr. Santosh Kumar Mishra²;

Research Scholar, Computer Science Department, MUIT, Lucknow, UP, India¹;

Assistant Professor, Computer Science Department MUIT, Lucknow, UP, India²

E-mail: pruthvi14390@gmail.com¹; sant7783@hotmail.com²

ABSTRACT

Using cloud storage customers can remotely store their data but cloud data storage redefines the security issues related to the user outsourced data. Single service provider is not sufficient for providing the high security to the customer's outsourced data. In order to achieving better privacy and availability user's data can be divided into the number of data blocks and can be distributed over the available service provider's. For successful retrieval of whole user data threshold number of service provider's should take part into it. In this paper, we proposed a secured cost-effective multi-cloud storage model in cloud computing which provide cost effective solution for the users outsourced data privacy and availability.

Cloud computing is sharing various computing resources rather than having local servers or personal devices to handle applications over internet. There are different types of cloud services namely, Software as a Service, Platform as a service and Infrastructure as a service. The Multi-Cloud or 'Cloud-of-Clouds' has emerged as key solution to various obstacles faced in single clouds. Multi cloud is highly required due to the fact that sensitive data should not be entrusted to a single cloud, to avoid dependency on just one cloud provider. Hence switching the cloud computing from single cloud to multi-cloud is mandatory to fulfill data security. Existing Multi-cloud types include Intra Cloud, Hybrid cloud, Federated Clouds and Multi-Cloud. There are several approaches available to enhance security in multi-clouds. Data to be stored is split into various blocks and distributed among different cloud storage providers in a redundant way. Other methods include holomorphic encryption,

Attribute based Encryption (ABE), building a Multi-cloud database model (MCDB) etc.

Keywords: Cloud Computing, Data Sharing, Cloud Service Provider, Data Security, multi Cloud.

1. INTRODUCTION

Cloud computing is basically cost effective and on demand service offered to the clients. The cloud is a multi-tenant environment, which implies that a single architecture has various clients' applications and data. Multi-cloud is the combination of public, private or managed clouds, including managed services or service providers. In today's world information storage or sharing means business. In the single cloud storage data remains on the centralized storage which can be easily accessed by the malicious insiders. Companies should start considering working with more than one cloud provider at a time - for cost savings, performance, disaster recovery and other reasons. Most business organizations share most of their data with either their clients or suppliers and consider data sharing as a priority [1]. Through data sharing, higher productivity levels are reached. With several users from various organizations contributing to the cloud data, cost and time spent would be less compared to the traditional ways of manually sending and sharing data, which often led to the creation of out-of-date and redundant documents [1].

Although many cryptographic data slicing methods [2], [3], [4] have been proposed as the main problem arises in the insider's access to stored data. Insiders are the trusted secondary admin or managers who maintains the third party server with the same authorization as the admin. Since the third party servers or

infrastructure has been used to store any sensitive information. Administrators and third parties manage the infrastructure as they have remote access to the servers. Multi-Cloud is the utilization of various computing services in a single heterogeneous architecture.

Multi- Cloud Storage means the utilization of various cloud storage services using a single web interface rather than the defaults provided by the cloud storage vendors in a single heterogeneous architecture. Multi-Cloud data systems have the capacity to enhance data sharing and this aspect will be significantly of great help to data users. It enables data owners to share their data in the cloud. In any cloud computing model, security is regarded as the most crucial aspect due to the sensitivity and delicacy of the user's information or data stored in a cloud. The idea on reducing the risk for data in a cloud is the simultaneous usage of multiple clouds. Multi cloud computing creates a large number of security issues and challenges. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. Different services are accessed from the multi-cloud user. The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. Various approaches for multi-cloud security differ in portioning and distribution patterns, technologies, cryptographic methods and security levels. The assessment of different methods with regards to legal aspects and compliance implications is important.

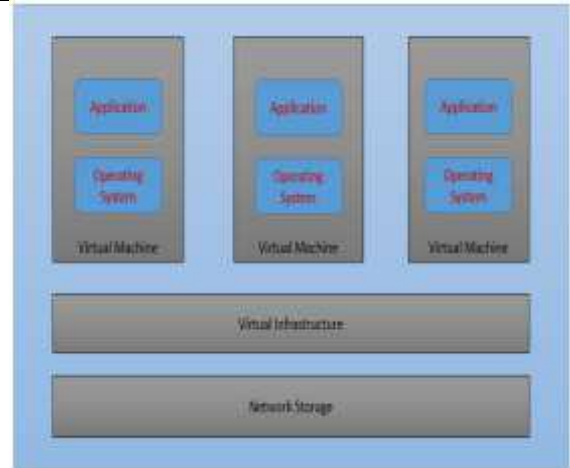
CLOUD COMPUTING TECHNOLOGIES

There are several cloud computing technologies, which makes the cloud computing flexible are listed below:

- Virtualization
- Service-Oriented Architecture (SOA)
- Grid Computing
- Utility Computing

Virtualization

Virtualization is a technique, which shares the single instance of the resource among multiple organizations or the users. The logical name is assigned to a physical resource and the pointer is provided to that physical resource, when demanded. The multiuser architecture offers virtual isolation among multiple users. Therefore the organizations use and customize the applications and have its own instance running. The virtualization technology is shown in Figure (a).



Figure(a) Virtualization Technique in the Cloud

Service Oriented Architecture (SOA)

Service Oriented Architecture (SOA) use the applications as a service for other type of vendors, product or technology. Hence, it is possible to exchange the data between the applications of different vendors without any additional programming services.

Grid Computing

Grid computing refers to the distributed computing in which the groups of computers from multiple locations are connected to each other to achieve the common objective. These types of resources are heterogeneous in nature and are geographically distributed. The process in grid computing breaks the complex task into smaller number of tasks. These smaller tasks are distributed to CPUs that reside within the grid. The Grid Computing technology in cloud is shown in Figure (b).

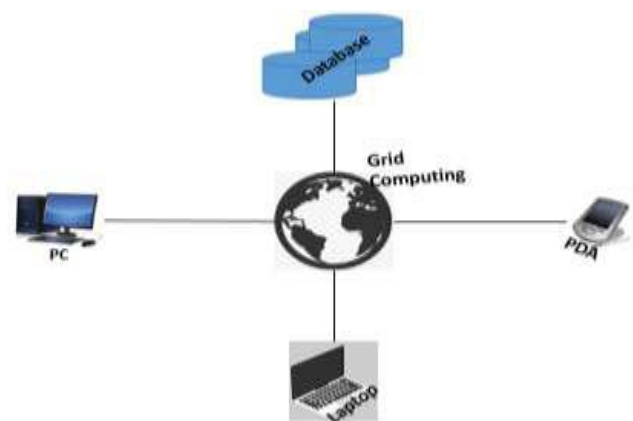


Figure (b) Grid Computing Technology in the Cloud

Utility Computing

The utility computing is based on the Pay as you use model. The utility computing is a metered service and offers a computational resource on demand, whenever needed. The cloud computing, grid computing and the

managed IT services are all based on the concept of utility computing.

2. LITERATURE SURVEY

Sr. No.	Author Name	Implementation Details	Benefits	Technique
1	Minqizhouet al.	Analyze privacy acts which are outdated	Multi-location issues were discussed	Availability, Confidentiality, Data Integrity, Control and Audit are addressed
2	Mohammed A. Al Zainet.al.	Architecture of MCDB to handle data in multi-clouds	Development of a model to handle data in multi-cloud	MCDB model
3	MdKausar Alam etal.	Multi-clouds and use of Shamir's Secret sharing algorithm	Protection of data in cloud	Shamir's Secret Sharing algorithm
4	Eman M. Mohamedet al.	Speed, higher security and performance were taken as parameters	Encryption time was least in AES	Analyzed 8 Encryption algorithms
5	Amandeep Kaur etal.	RSA algorithm for data storage	Data security	RSA algorithm
6	AbdulRazaque et al	Using polynomial, secret points are computed	Data sharing in Multi-clouds	Lagrange polynomial of the fPorm: $f(x) = \sum_{i=0}^2 Y_i(l)$
7	R.K.Banyal et al.	Centralized access control for cloud resources	Security of cloud is ensured	Dynamic Trust Based Access Control Frame work (DTBAC)
8	TaraSalman et al.	Security requirements in Multi-Cloud, Its architecture	Data security in multi-clouds is strengthened	Distribution based, Cryptography based and Hybrid based solutions
9	Ganesh A. Prajapatiet al.	Byzantine Protocols, Secret Sharing Algorithm are implemented	Security is enhanced	Dep Sky System

10	Veena Khandelwal et al.	Treating data privacy as 'Normal', 'Sensitive' and 'Critical' levels and split the user data into chunks and give them to CSP's to provide Database as a Service	Client privacy and data distribution	Database as a Service and categorization of user data
11	He Kai,Huang Chuanheet al.	Applied holomorphic cipher text verification	Multi-cloud storage and recoverable coding approach	Public batch data Integrity auditing protocol
12	AbdulRazaque et al	Using polynomial, secret points are computed	Data sharing in Multi-clouds	Lagrange polynomial of the fPorm: $f(x) = \sum_{i=0}^n Y_i(l)$
13	A. Manimaran et al.	Authentication without compromising a user's private information. The data integrity verification is done by using a Third party auditor. It used Anonymous ID assignment based data sharing algorithm	Data integrity verification is done	efficient based privacy preserving authentication protocol(EAPA)and Anonymous ID assignment based data sharing algorithm

Cloud computing generally refers to the online services like online software application, data storage and processing powers which are pay per use services. Cloud computing is mostly use for dynamically increase the processing capabilities or add capabilities. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

A huge amount of data being retrieved from geographically distributed servers, and non-localized data handling, creates such a change in technological. One of the prominent services provided in cloud computing is the cloud data storage.

In cloud computing, customers have to pay for data storage services. This service does not only provides flexible and scalable data storage, it also provides customers with the benefit of paying only for the block of data they needs to store for a particular amount of

time, without any worries about of efficient storage mechanism and maintainability issues and challenges with large amounts of data storage.

Along with these various advantages, cloud data storage also redefines the security issues based on customer's outsourced data (Data which is not stored on customer's server). Since cloud service providers are separate market entities. Security and privacy are most common issues need to be addressed in cloud computing. Cloud computing has done major advancements to the IT industry. Cloud computing brought up rapid enhancement in to the industries and business. The most important and common security and privacy issues related to the user outsourced data which is processing on remote machine that are not managed by customer. With cloud computing user can see virtual infrastructure built on non-trusted physical hardware and operating environment. The cloud

customer should be able to control and manage the different privacy techniques important to protect sensitive outsourced data.

3. EXISTING SYSTEM

In the cloud computing, the data is stored on an autonomous business party that provides data storage as a subscription service. The users have to trust the cloud service provider (SP) with security of their data. Obtaining information from a third party is much easier than from the creator himself.

Following the pattern of paradigm shift, the security policies also evolved from the conventional cryptographic schemes applied in centralized and distributed data storage, for enabling the data privacy. Many of the cryptographic approaches have been proposed for hiding the data from the storage provider and hence preserving data privacy.

The user's identity is also detached from the data, and claim to provide public auditing of data. These approaches concentrate on one single cloud service provider that can easily become a bottleneck for such services. The sole crypto-graphic measures are insufficient for ensuring data privacy in cloud computing. In cloud storage needs a hybrid model of privacy enforcement, distributed computing and complex trust ecosystems.

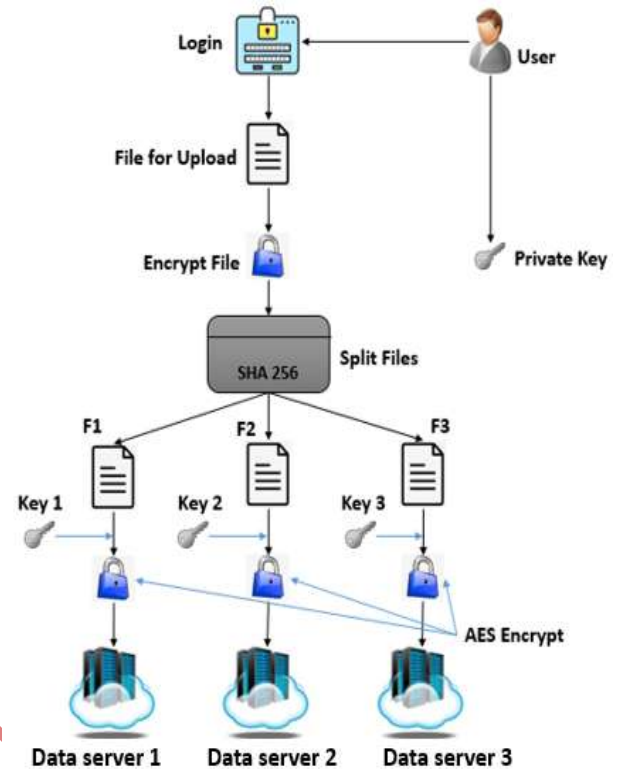
To provide users with better and fair chances to avail efficient security services for their cloud storage at affordable costs, our model distributes the data pieces among more than one service providers, in such a way that no one of the SPs can retrieve any meaningful information from the pieces of data stored on its servers, without getting some more pieces of data from other service providers. Therefore, the conventional single service provider based cryptographic techniques does not seem too much promising.

4. PROPOSED SYSTEM

The proposed methodology includes a number of modules which perform major operations of storing a file into multiple cloud servers. Every file undergoes processing before it is stored in the file.

The proposed methodology guarantees the file slicing with index based parts gets encrypted and stored on the Multi-Cloud. This method ensures the file cannot get access without the knowledge or permission of the owner. Data owner uploads the file through the proposed framework interface. The framework uploads the file in the local machine. The framework splits the file with its indexes assigned and encrypts each part of the file using the secret or private key provided by the

owner. Each part of the encrypted file gets stored in the owner's machine and then transferred to the multi-cloud server. The receiver sends the decryption request to the owner or the owner can share the required credentials through Bring Your Own Secure Channel (BYOC) or out of band procedure.



Proposed Architecture Secure Multi Cloud Storage

The receiver enters the credentials through the framework interface. The framework retrieve the file parts and each parts get decrypted, merged and stored the receiver's machine. The major contributions, as described in this report are as follows. The unique feature of this system is to protect the data access from malicious insiders and to protect the datacenters information from malicious files .In addition it also has provision the index based cryptographic data slicing in Multi-Cloud storage services to reduce the file merging conflicts and on demand cost for the customers. It make clients better and fair opportunities for decision making process to choose multi-cloud storage services for secure sharing of data based on trust. The proposed work guarantees that file slicing is based on the number of storage services. More than four cloud storage services are used for confidentiality and none of the Cloud Storage Service Providers can retrieve meaningful information from the pieces of information

stored on its servers, without getting some more bits of data from other storage service providers.

CONCLUSION

There are different analysis that are conducted to look into the security of multi cloud and a classification about data at rest and data in transit is required for efficient handling of data security features. Each approach discusses briefly about the algorithm used and the architecture needed to enhance the security. A novelty in multi-cloud security should have the flavors of cryptographic functions combined with the selection of best algorithm for encryption of data together with Deduplication measures to ensure one copy of the data is stored thereby ensuring data Integrity and ensure availability.

FUTURE SCOPE

There are various encryption algorithms which impose greater security on the files which can be used in this specific use case, as encryption is made modular allowing the system to be improvised with more advanced encryption algorithms developed in the future. The process can be made Highly Available (HA) by backing up the contents of each of every part in different servers just to make sure that if one server fails the user must not lose the content that is stored on that particular server. Furthermore, better key management strategies can be adopted to manage the keys used for encryption.

5. REFERENCES

- 1) DananThilakanathan, ShipingChen,Surya Nepal and Rafael A.Calvo —Secure Data Sharing in the Cloudl. In Security, Privacy and Trust in Cloud Systems, Springer Berlin Heidelberg, 2015,(pp. 45-72).
- 2) Benjamin Fabian, Tatiana Ermakova,PhilippJunghanns —Collaborative and secure sharing of healthcare data in multi-cloudsl. Information Systems, Volume 48 Issue C, 2015,pp 132-150
- 3) Balasaraswathi, V. R., &Manikandan, S. (2014).l Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approachl. In Advanced Communication, International Conference on Control and Computing Technologies (ICACCCT), 2014 on (pp. 1190-1194). IEEE.
- 4) Mazhar Ali, Revathi Dhamotharan, ErajKhan, SameeU. Khan, Athanasios V.Vasilakos, KeqinLi, Albert.Y.Zomaya —SeDaSC: Secure Data Sharing in Cloudsl, Systems Journal, IEEE, Volume: PP, Issue: 99, 2015, pp 1-10.
- 5) Minqi Zhou, Rong Zhang, WeiXie, WeiningQian, AoyingZhou, “Security and Privacy in Cloud Computing: A Survey”, 2010 Sixth International Conference on Semantics, Knowledge and Grids.
- 6) Mohammed A. Al Zain, Ben Soh and Eric Pardede,”MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing”, Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia.
- 7) Eman Mohamed, Hetem S. Abdelkar and Sherif El-Etrib.”Enhanced data Security Model for Cloud Computing”, 8th International Conference on Informatics and system (INFOS2012)—May 2012.
- 8) MdKausarAlam, SharmilaBanu K,” An Approach Secret Sharing Algorithmic Cloud Computing Security over Single to Multi Clouds”, International Journal of Scientific and Research Publications, Volume 3, Issue4, April 2013.
- 9) Amandeep Kaur, Sarpreet Singh. “An efficient data storage Security Algorithm Using RSA algorithm”.—International Journal of Application or Innovation in Engineering & Management (IJAIEM) March 2013.
- 10) Abdul Razague, saty Siva VarmaNadimpalli, Suharsh Vommina. “Secure Data Sharing in Multi-Clouds”.
- 11) R.K. Banyal, V.K. Jain, Pragya Jain, “Dynamic Trust Based Access Control Frame Work for Securing Multi-Cloud Environment”, ACM/ 978-1-4503-3216-3/14/11.
- 12) Tara Salman. “On Securing Multi-Clouds: Survey on Advances and Current Challenges”, Nov 2015.
- 13) Zissis, D &Lekkas, D 2012, „Addressing cloud computing security issues”, Future Generation computer systems, vol. 28, no. 3, pp. 583-592.
- 14) Zhou M, Zhang R, Xie W, Qian W & Zhou A 2010, ‘Security and privacy in cloud computing: A survey’, Sixth International Conference on Semantics Knowledge and Grid (SKG), 2010 pp. 105-112.
- 15) Tirthani N &Ganesan R 2014, ‘Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography’,

- IACR Cryptology ePrint Archive, vol. 2014, p. 49.
- 16) Xu G, Yu M, Cheng J, Li L & Shi Y 2013, 'Data Sampling Algorithms for Data Integrity Verification in Cloud Storage', International Journal of Advancements in Computing Technology, vol. 5, no. 9
- 17) Arockiam, L & Monikandan, S 2013, „Data security and privacy in cloud storage using hybrid symmetric encryption algorithm“, International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 8, pp. 3064-3070.
- 18) Wang Liang-liang, Chen Ke-fei, Mao Xian-ping, Wang Yong-tao —Efficient and Provably-Secure Certificate less Proxy Re-encryption Scheme for Secure Cloud Data Sharing| Journal of Shanghai Jiaotong University Volume 19, issue 4, 2014 pp. 398-405.
- 19) Peng Xu, Xiaqi Liu, Zhenguo Sheng, Xuan Shan, Kai Shuang —SSDS-MC: Slice-based Secure Data Storage in MultiCloud Environment| 11th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE), 2015, pp 304-309.
- 20) Shungan Zhou, Ruiying Du, Jing Chen, Hua Deng, Jian Shen, Huanguo Zhang —SSEM: Secure, Scalable and Efficient multi-owner data sharing in clouds|, China Communications IEEE, Volume 13, issue 8, 2016, pp 231-243.
- 21) Ibrahim Abdullah Althamary, Talal Mousa Alkharobi —Secure File Sharing in Multi-Cloud using Shamir's Secret Sharing Scheme, Transactions on Network and communications Vol 4 issue 6, 2016, pp 53-67.
- 22) [10] Maha Tebaa, Said El Hajji —From Single to Multi-Clouds Computing Privacy and Fault Tolerance|, Science Direct (ELSEVIER), International Conference on Future Information Engineering, (2014), pp 112-118.
- 23) Yuuki Kajiura, Shohei Ueno, Atsushi Kanai, Shigeaki Tanimoto, Hiroyuki Sato —An Approach to Selecting Cloud Services for Data Storage in Heterogeneous-Multi cloud Environment with High Availability and Confidentiality Autonomous Decentralized Systems| (ISADS) IEEE Twelfth International Symposium, 2015, (pp 205 – 210).
- 24) Dr. K. Subramanian, F. Leo John —Data Security in Single and Multi-Cloud Storage- an Overview| International Journal of innovative Research in Communication Engineering 2016 pp 19046-19052.
- 25) Alycia Sebastin, Dr. L. Arockiam —A Study on Data Security Issues in Public Cloud|, International Journal of Scientific and Technology Research Volume 3 Issue 5 May 2014 pp 144-146.
- 26) B. Rex Cyril, Dr. S. Britto Ramesh Kumar —Cloud Computing Data Security Issues, Challenges, Architectures and Methods-A Survey| International Journal of Engineering and Technology (2015).