International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

Available online: www.ijmrset.com e-ISSN: 2394-8752, p-ISSN: 2394-8791

Volume-03, Issue-11, November 2016

Data Security in Single and Multi Cloud Storage–An Overview

Dr.K.Subramanian[1], F. Leo John* [2]

Assistant Professor, PG and Research Dept. of Computer Science, H.H The Rajah's College, Pudukkottai, India[1]

Research Scholar, P.G and Research Dept. of Computer Science, JJ. College of Arts & Science (Autonomous), Pudukkottai, India[2]

ABSTRACT:In the modern era of computing, Cloud computing will play a major role in the Internet of Services. Although many cloud service models are there, Infrastructure as a Service (IAAS) has become the foundation of the future Internet of Services (IoS). Many advantages of cloud computing attracts the individuals and organization to move their data from remote to cloud servers. Cloud Providers mainly focus on delivering services and provides a lesser focus in data security and privacy which is the main aspect in cloud computing. Since the single cloud storage does not fulfil the demands of the individuals and organizations, a move towards multi-cloud storage has been emerged. This report offers an overview of motivation of attackers, various techniques and its limitations made to protect information security in single and multi-cloud storage. In addition, this paper also explains the common challenges in adopting single and multi-cloud storage services. This work provides a better solution in designing multi-cloud architecture and key consideration in decision making process for the individuals and organizations in the adoption of better cloud storage service.

KEYWORDS: Cloud Security, Data Security, Single Cloud Storage, Multi-Cloud Storage

I. Introduction

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.Napoleon once broadly said, "War is a 90 % data." There are 3 things to notice regarding this statement. First, it's as true today as it was 200 years ago. Second, it's equally applicable to business because it is to the battle ground. Third, 90% are conservative; today's businesses virtually are data. The stakeholder's primary reason for moving to the cloud is to reduce costs. Businesses big and small are turning to cloud computing systems to forge leaner, more efficacious and efficient systems. In cloud computing, security may be assured to data or information and files or records which has to be stored in the cloud storage. Through data sharing, higher productivity levels are achieved.

While information security has been a topic of extreme importance since the beginning of time, the present nature of today's internet has accelerated the importance of this area to a new and critical level. It is absolutely vital, that in today's world, one must have confidence that secrets, whether they are composed of credit card numbers, personal data or information of national importance, remain secret as they pass through several elements encountered along the communication path from source to destination.

Data or information relates to the database in which one specific column or attribute is to be secured. In order to store the data securely, many cryptographic techniques are available. On the other hand files are the unstructured data in various formats which are readily available in adopting the cloud storage service. Nearly all the cloud storage providers are maintaining good infrastructure to store all types of file formats. Unfortunately, many storage providers provide lesser focus on security to support all file formats and in their architectures.

Most of the providers will guarantee 99.9% security and privacy is possible in Service Level Agreement (SLA), but none of the provider or cloud broker has an integrated tool or framework to auto detect those challenges. The file security plays a major role in cloud storage. As aforesaid various file formats are available in various sizes, it's not an easy task for a service provider to give protection or provision to upload for all file formats. Some of the file formats, especially video files may not supported by providers framework or tools. There are three main reasons that makes cloud provider to do so. They are size, internet traffic and cost.[19]The makeup of internet traffic itself is changing. Historically, File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP) and peer to peer traffic are already available. Today video is already dominating the mix and by 2020, it is estimated that video will represent more than 98 percent of all consumer traffic. This shift has broad implications. In the past, IT department's job was to build a data

and voice network that carried some video. But from now on, the IT department's job was to build a video network that might carry some data and some voice. Safe to say, video files not only alters the form and behavior of traffic on networks, merely it is pushing cloud service providers to modify the way they conceive, plan, and operate networks.
[17] A similar comparison to data security in a cloud is in banks where a client deposits his cash bills into an invoice with a bank and so no longer induce a physical valuable thing in his ownership. The customer will depend on the technology and the integrity of the bank to protect his virtual valuable thing. Likewise, there will be an increase in the bit of cloud customers to store the data in physical locations out of their reach but with a trusted provider.
The rest of this paper is organized as follows. Chapter 2 discusses the related works of the secure data sharing in the single and multi-cloud storage with its limitations.Chapter 3 describes the motivation of the attackers and the need for effective data security. Chapter 4 explains the recent threats and solutions in cloud computing and Chapter 5 concludes the report.

II. Related work

Privacy and security for cloud storage are generally a wide area of research. Numerous academic interrogations have been conducted to identify the potential security issues about this subject. Ref [1], proposed the multi-cloud storage architecture which features attribute-based encryption for selective access authorization and cryptographic secret sharing in order to scatter data in multiple clouds. In this approach standard procedure is not used to protect the keys and user revocation needs heavy computation. Ref [3], provides a multi-cloud storage architecture which features Advance Encryption Standard (AES) procedure for data protection. This approach uses two clouds for storing the files and one private cloud for storing the metadata of the files stored such as passwords, secret keys and encrypted file access paths. Data breach threat is possible in this approach since the data persist in the two clouds for longer time if service provider colludes. Also file access paths are changed periodically it requires heavy computation in decryption process. In [15] an architecture has been proposed that uses cryptographic data splitting to store the data in the multi-cloud server. Since the data stored in the multi cloud was not encrypted various threats are possible in this approach especially data breach and system vulnerabilities. Ref [4] provides an architecture and a standard procedure for secure data sharing in cloud. This approach does not use multi-cloud storage. Most of the security operations are maintained by third service provider it requires high trust to use this approach. Ref [5] proposed the proxy re-encryption scheme which does not need the public key certificates to guarantee validity of public keys and solves the key escrow problem in identity-based encryption. This approach uses bilinear pairing for proxy re-encryption but the computational cost of proxy re-encryption scheme is high when compared to standard operations in finite fields. To reduce the computational overhead of bilinear paring [12] proposed a mediated certificate less proxy re-encryption scheme which solves the key escrow and user revocation problem. In this scheme cloud generates the public-private key pairs for all the users and transmits the public key to all the sub users. From the security perspective it is not recommended to shift the key generation process to shared multi-user cloud environment.

The restrictions of single cloud storage are given in [21].Various Multi-cloud data storage approaches with its pitfalls and weak spots, either in terms of security, compliance and feasibility had been hashed out in [18]. To enforce the privacy and security protection of data in the cloud [6] proposed Slice-based Secure Data Storage in Multi-Cloud Environment an architectural prototype using AES encryption. The only drawback in this approach is it doesn't support video files and it takes larger time when the file size is large since the file slicing size is fixed.

III. CLOUD SECURITY ISSUES AND ATTACKERS MOTIVATIONS

Cloud computing security or cloud security involves PC security, Network security, and most completely data or information security. It implies a broad set of policies, innovations, and controls sent to secure data, applications, and the associated infrastructure of cloud computing. For any commercial enterprise, secure digital data are increasingly valued for being truly a record that serves as a magnificent confirmation of reality.

A. ATTACKERS MOTIVATIONS

There are two types of information: information somebody needs to take and everything else. Most security experts today don't see the motivations behind data theft; [20] in 2014, Harvard Business Review uncovers that various government and individual case studies have set up that insiders who intentionally take participate in cyber-attacks have an expansive range of inspirations. Some of them are financial gain, revenge, desire for recognition and power, move to blackmail, true to others in the organization and political convictions.
Figure-1 shows the architecture of private cloud which is a shared and multi-tenant environment built on a highly effective, automated and virtualized infrastructure. In single cloud storage security managers put controls in place that protect the data that is most valuable to them, equally opposed to information that is most valuable to criminals.

This means that control management is regularly defective and security experts frequently leave dangerous data, data associated with legal or consistence commands, and certain cases of intellectual property unprotected and vulnerable. In order to overcome the above challenges Multi-Cloud storage with high availability and security features has been emerged.

B. RECOMMENDATIONS FOR THE CLOUD SERVICE PROVIDERS

With a specific end goal to upgrade the security aspects of the Multi-Cloud storage a consideration ought to be taken in planning security system or model. This paper summarize the following requirements can be considered in building the effective architecture to meet the requirements of cloud consumers are given below.

a) Decentralization of encryption and decryption of storage.

b) Removal of unwanted files frequently.

c) Encryption resources such as keys, hash algorithms, certificates, and digital signatures are dynamically changed regularly.

d) Finally centralized key management.

C. RECOMMENDATION FOR CLOUD CONSUMERS

. In contrast the clients should note the following points when moving to public cloud. They are as follows:

a) Avoid cloud brokers and third party cloud service providers.

b) Thorough investigation of how the cloud provider secure its system.

c) Find out all the provider's employee or contractors can access the system.

d) Find out who will monitor the customer's data.

e) Have a written plan for security events,

g) Find out how data will be securely returned in the event of cancellation of cloud service

h) And check for the data deletion when the user opts out of the subscription.

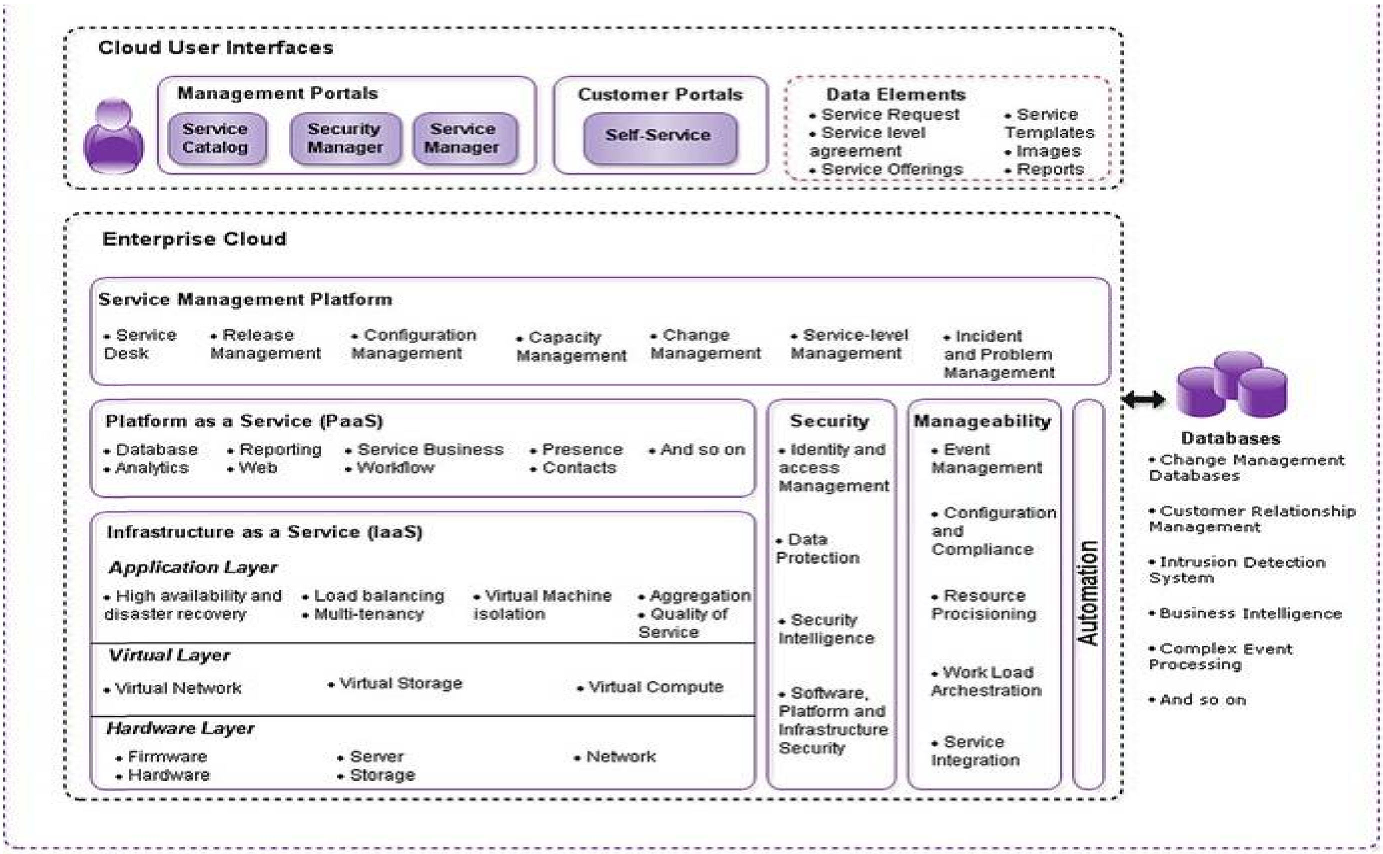

Figure-1Cloud Architecture

IV. THREATS

There are number of types of privacy and security threats in the cloud. The following describes the summary of various threats in cloud computing and their impact on organization.

a) **Data Breach**: Any kind of information viewed or stolen by unauthorized user. It is caused due to the result of human-error, application vulnerabilities or poor security practices. Corporate Network and Telecom operator organization gets affected by this attack. These attacks can be minimized by implementing multifactor authentication and encryption.

b) **Insufficient Identity, Credential and Access Management:** This attack is caused due to the absence of identity verification, lack of analyzing the quality and absence of resource management. Any organization that has maintained centralized storage mechanism containing data secrets gets affected by this attack. This risk can be minimized using De-provisioning of access to resources and monitoring the resources.

c) **Insecure Interfaces and APIs:** Cloud computing providers uncover a set of programming User interfaces (UIs) or application programming interfaces (APIs) that clients use to manage and collaborate with cloud service. The main resource is an IP address which can be accessed outside the trusted organizational limit. These properties will be the Target of heavy attack. Any organization that has flaws in data flows and architecture or system design in the development life cycle. Security-specific code reviews and rigorous penetration testing can be used to prevent these attacks.

d) **System Vulnerabilities:** Framework vulnerabilities are exploitable bugs in projects that aggressors can use to invade a PC framework with the end goal of taking information, taking control of the framework or upsetting administration operations. Highly regulated organization like financial and government institutions are the main target of these attacks. This attack can be minimized by Cleaning up after the successful system attack, document the patch work and reviewed by technical team.

e) **Account Hijacking:** Account or service hijacking isn't new. Attack strategies like phishing, fraud and exploitation of software package vulnerabilities still reach results. If an attacker gains access to your credentials, they will listen in on your activities and transactions, manipulate information, come falsified info and direct your purchasers to illegitimate sites. E-commerce organization when credentials are shared gets affected by these attacks. The only way to prevent this attack is monitoring all account activities.

f) **Malicious Insiders**: A malicious insider risk to an association is a present or previous employee, contractual worker, or different business partner who has or had approved access to an organization’s network. A malicious insider, such as a cloud service administrator, can access potentially sensitive information. Cloud Service providers have huge impact on this attacks. This can be minimized by rein shared accounts and better user tracking activities periodically.

g) **Advanced Persistent Threats:**Advanced Persistent Threats (APTs) are related to things that slowly feed off of and weaken other things This computer attack gets into a system to establish a solid, secure place to start winning or gaining power in the computing infrastructure of target companies from which they illegally take some data and intellectual property. Any organization which has unsecure networks can gets easily affected by this attack. Awareness programs that are regularly reinforced.

h) **Data Loss:** Data stored within the cloud will be lost for reasons aside from malicious attacks. An accidental deletion by the cloud service provider, or worse, a physical catastrophe like a fireplace or earthquake, will cause the permanent loss of client knowledge. Any organization such as banking and health care are highly targeted for this type of attack. Adequate measures to back up data, following best practices in business continuity and disaster recovery may reduce this attack.

i) **Insufficient due Diligence**: A complete study of business is needed before signing a contract. A company that rushes to adopt cloud technologies and opt for CSPs while not performing due diligence exposes itself to a myriad of business, financial, technical, legal and compliance risks. Any organization that has not study the compliance of new adoption of the cloud. Customers must understand the risk when adopting new technology.

j) **Denial of Service:** Denial-of-service (DoS) attacks are attacks meant to stop users of a service from having the ability to access their information or their applications. Distributed denial-of-service (DDoS) attacks—causes an intolerable system delay and leaves all legitimate service users confused and angry about why the service isn't responding. Cloud Service Providers (any) and private Data centers can be affected by this attack. Auto Detection or monitoring tool is required when website becomes slow.

Below table describes the various research approaches used to protect the data and its limitations in cloud storage

Table-1 Existing Approaches used to protect data in single and Multi-Cloud Storage

S.No	Existing Approach	Technique Used	Limitations	Possible Attacks
1	[1]. Collaborative Secure Sharing of Health Care Data in Multi-Cloud	An architecture with Attribute Based Encryption and cryptographic Data Sharing	No standard procedure is used to protect cryptographic keys. User revocation needs heavy computation	Insufficient Identity Credential and Access Management, Data Breach
2	[3] Enhanced Security for multi-cloud storage using cryptographic data splitting with dynamic approach	Cryptographic data splitting is used to store data in two clouds.	Service Provider Colluding attacks is allowed since data persist in the cloud for a long time	Malicious and data breach attacks
3	[4]. Secure Data Sharing in Clouds	A methodology with symmetric encryption is proposed with sharing a part of the key with users and the other part in the server	Most of security operations are maintained by third party. No monitoring frame works for third party.	Account hijacking and data breach.
4	[5]. Efficient and provably –secure certificate less proxy re-encryption scheme for secure cloud data sharing.	An architecture with public key encryption scheme is used to secure data in the single cloud.	Trusted authorities are used with monitoring framework. Bilinear parings are used which in turn increases the computation overhead.	Malicious and Data Breach attacks
5	[6] Slice- Based Secure Data Storage in Multi-Cloud Environment	An architectural framework with cryptographic data slicing technique is proposed for storing the file in Multi-Cloud.	Framework is not fully automated. Additional burden to the customers.Meta table is used for storing the file information and slices. Video files not supported	Account Hijacking and Insufficient identity credential and access management
6	[15] A secured cost-effective Multi-Cloud Storage	A model with data slicing technique is proposed for storing the file in multi-cloud storage.	Since data is not encrypted and also not monitored gets stored in multi cloud various attacks are possible.	Data Breach, Malicious,System vulnerabilities

V. CONCLUSION

This work describes the overview of Multi-Cloud storage approaches which explains the techniques, challenges and its limitations. Many similar approaches has been proposed but there is a lack of improvement in technical approach. In real time it is a tedious process for individuals, and service providers to fulfil their demands.

REFERENCES

[1].Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*, *48*, 132-150.

[2]. Thilakanathan, D., Chen, S., Nepal, S., & Calvo, R. A. (2014). Secure data sharing in the cloud. In *Security, Privacy and Trust in Cloud Systems* (pp. 45-72). Springer Berlin Heidelberg.

[3]. Balasaraswathi, V. R., & Manikandan, S. (2014). Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach. In *Advanced Communication, Control and Computing Technologies (ICACCCT), 2014 International Conference on* (pp. 1190-1194). IEEE.

[4] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. KhanAthanasios V. Vasilakos (2014). *SeDaSC: Secure Data Sharing in Clouds,* Systems Journal, IEEE pp 1-10.

[5]. WANG Liang-Liang, CHEN Ke-Fei, MAO Xian-ping, WANG Yong-TaoEfficient and Provably-Secure Certificateless Proxy Re-encryption Scheme for Secure Cloud Data Sharing *Journal of Shanghai Jiaotong University (2014)* Volume 19, issue4, pp 398-405.

[6]. Peng Xul, 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.

[7]. Yuuki Kajiura, Shohei Ueno, Atsushi Kanai, Shigeaki Tanimoto, Hiroyuki Sato An Approach to Selecting Cloud Services for Data Storage in Heterogeneous-Multicloud Environment with High Availability and Confidentiality *Autonomous Decentralized Systems (ISADS 2015) IEEE Twelfth International Symposium* (pp 205 – 210).

[8]. Tatiana Ermakova,Benjamin Fabian Secret Sharing for Health Data in Multi-provider Clouds*Business Informatics (CBI), 2013 IEEE 15th Conference (2013)* pp 93-100.

[9]. Hendrik Graupner, Kennedy Torkura, Philipp Berger, Christoph Meinel Secure Access Control For Multi-Cloud Resources *Local Computer Networks Conference Workshops (LCN Workshops), 2015* pp 722-729.

[10].Hazila Hasan, Sultan Abdul Halim Muadzam Shah Secured Data Partitioning in Multi Cloud Environment *Information And Communication Technologies (JWICT), 2014* pp146-151.

[11]. Xu, L., Wu, X., & Zhang, X. (2012, May). CL-PRE: A certificate less proxy re-encryption scheme for secure data sharing with public cloud. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security* (pp. 87-88). ACM.

[12].Seo, S. H., Nabeel, M., Ding, X., & Bertino, E. (2013, September). An efficient certificateless encryption for secure data sharing in public clouds. *Knowledge and Data Engineering, IEEE Transactions on*, *26* (9), 2107-2119.

[13].Khan, A. N., Kiah, M. M., Madani, S. A., Ali, M., & Shamshirband, S. (2014, May). Incremental proxy re-encryption scheme for mobile cloud computing environment,*The Journal of Supercomputing*, *68* (2), 624-651.

[14].Michael O. Rabin (1989, April) Efficient Dispersal of Information Security, Load Balancing, and Fault Tolerance *Journal of Association for Computing Machinery* pp335-348

[15].Yashaswi singh,Farah Kandah,Weiyi Zhang A Secured Cost-effective Multi-Cloud Storage in Cloud Computing,IEEE INFOCOM workshop on Cloud Computing(2011) pp 619-624.

[16].Top Threats Group, "The Treacherous 12 Cloud Computing Top Threats in 2016",http://www.cloudsecurityalliance.org.

[17]. Borko Furht, Armando Escalante "The Handbook of Cloud Computing",Springer Publications 2012.

[18].Jens-Matthias Bohli,Nils Gruschka,Meiko Jensen,Luigi Lo Lacono and Ninja Marnau,"Security and Privacy-Enhancing Multicloud Architectures" IEEE Transactions On Dependable and Secure Computing(2013) pp-212-224.

[19].Venkata Josyula, Malcom Orr, Greg Page,"Cloud Computing:Automating the Virtualized Data Center" Cisco Press 2012.

[20].www.hbr.org

[21].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)pp112-118.

[22].Alycia Sebastin,Dr.L.Arockiam A Study on Data Security Issues in Public Cloud, *International Journal of Scientific and Technology Research(2014).*

[23].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).

BIOGRAPHY

1. Dr.Subramanian Krishnasamy is currently working as an Assistant Professor in H.H The Rajah's College. His area of interest includes Data Mining, Networking, Cloud Computing, Network Security, Big Data and so on.

2. Mr. Leo John is a part-time research scholar in Computer Science JJ.College of Arts and Science pudukkottai. His area of interest includes Cloud Computing, Unstructured Data Security in multi-cloud, cryptography and so on.