Security Issues and Solutions in Cloud Storage as a Service : A Review

YSR Gayatri*[1], Chandresh Parekh[2]

*[1]M.Tech. Department of IT & Telecommunication, Raksha Shakti University, Ahmedabad, Gujarat, India

[2]Asst. Professor, Department of IT & Telecommunication, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

Cloud computing (CC) is a fast growing business considering its attractive features and undeniable advantages at an affordable cost. The boon of immense flexibility, accessibility and availability of data of individual customers comes with attached security concerns. This review paper briefly introduces existing types of cloud services with emphasis on storage of data offered as a service. Data security is a big concern that can be detrimental to the growth of cloud users. The security issues in present day cloud storage have been reviewed. A cryptographic technique is suggested to enhance security with increased speed.

Keywords: Cloud Computing, Storage as a Service, Encryption Techniques

I. INTRODUCTION

The cloud computing (CC) is an information technology (IT) exemplar that enables ever-present access to system resources that can be configured and provide eminent services that can be accessed at a great rate with very less management effort, over the internet, in a shared pool [1]. Many businesses are moving to cloud to utilise the technological as well as economic benefits of cloud. Deployment methods of cloud are many. Popular deployment models used mostly are:

1) Private Cloud: When a cloud infrastructure is used for both personal and commercial use by an organization whether maintained and hosted either internally or externally. Though private cloud is very attractive and beneficial, the organizations using private clouds should keep in mind all the security issues which can be encountered and take appropriate countermeasures to prevent these vulnerabilities [1].
2) Public Cloud: A cloud that provides its services over the internet for the entire public use. Although the architecture is quite similar the security measures taken for both are pretty different for the services that are provided by the cloud service provider (CSP). Some cloud services are provided publicly such CSPs are amazon web services, oracle, Microsoft and Google [1].

3) Hybrid Cloud: That cloud deployment model which combines two or more cloud models in way that takes advantage of multiple types of cloud. This cloud allows a user to either increase the capacity of cloud service or its capability by using integration, aggregation or customization with another cloud service [1].

4) Others: Other cloud deployment models include community cloud, distributed cloud, multicloud and many more customized according to the needs of an organization or the user.

Mostly any cloud deployment model offers three standard services [1]. These are sometimes called cloud computing stack. This name is used because they build above one another [2]:

1) Infrastructure as a Service (IaaS): The basic service provided among all cloud computing services. With IaaS, one can lease IT infrastructure, which can be servers, virtual machines, storage spaces, operating systems from a cloud provider and meet costs as they arise [2].

2) Platform as a Service (PaaS): PaaS supplies an environment to develop software applications and test, deliver and manage them on-demand. PaaS is made for developers so that they can create web and/or mobile applications, without fretting about setting up or managing the much-needed infrastructure for development [2].

3) Software as a Service (SaaS): It is the service for an on demand supply of software applications via Internet on basis of a subscription. CSPs can host and manage these applications, underlying infrastructure and can handle maintenance if required. Users connect to the applications over the Internet, usually with the help of a web browser on their phone, tablet or PC [2].

4) Others: There are many more services offered by the cloud like which in general is referred as Everything as a Service (EaaS or XaaS) [1]. Such as Communication as a Service, Monitoring as a Service, **Storage as a Service** and many more.

With all these services and new technologies comes security issues as well which should be taken care of at every development and implementation stage. One such service as named above is Storage as a Service. The huge amount of data that is needed to be stored in the cloud is termed as big data and this service is Storage as a Service, provided by the Cloud Service Provider (CSP) [1]. The security issues and proper measures for this service are suggested in this paper so that the cloud environment can be made more secure and trustworthy for users and the CSPs.

II. STORAGE AS A SERVICE

The CSP owns and maintains the hardware and software required while user uses these facilities via web applications. Using cloud storage reduces the cost of establishing and maintenance. This storage is very efficient as it can be accessed any time and provides global scale to store and share data over internet [3]. In the enterprise, the vendors are advertising cloud storage as a suitable way to manage backups, mitigating risks, long term record retention and enhancing businesses' availability and integrity by targeting storage applications at secondary level. Small scale businesses which lack capital/personnel to handle an infrastructure of their own can use cloud storage as a good substitute [4]. This cloud storage has mainly three categories:

1) Object Storage: This storage mainly takes advantage of scalability and characteristics of metadata of object's storage. It can be used ideally where applications are made from scratch and are scalable and flexible and require importing of data for being used in analytics, backups or archives [3].

2) File Storage: When an application needs access to the files that are shared and a file system this storage can be used as it provides a Network attached storage (NAS) server. It can be used ideally where there are content repositories on huge scale, developing environment, media stores, or user home directories [3].

3) Block Storage: This storage type is similar to Direct attached storage (DAS) or a Storage area network (SAN). It is ideally used where high performance workload is there [3].

III. SECURITY ISSUES AND SOLUTIONS

All Cloud based file storage is becoming most expected way of sharing files in both workplace and on personal devices these days. All businesses are jumping in to have powerful cloud storage with its growing popularity and versatility. As the demand is going high for cloud storage the cloud service industries are also rising. Like with every other system as popularity and demand grows the security issues also rise [5]. Cloud's Storage services also have security issues as listed below:

A. Attack Surface Area

When data is maintained and is stored at more than one location threat of unauthorized physical access to the data is increased. Like in the case of disposing the old equipment, drives reuse, storage space reallocation. The manner that data is duplicated depends on which service level a customer has chosen and on the service that is provided [3].

Solution: To ensure confidentiality encryption techniques can be used. In case of disposing off the data on a disk, the method of crypto-shredding is suggested. The Crypto-Shredding method is the deletion of all the encryption keys available for that particular data purposefully. This stays till someone uses brute force attack or till the encryption system is broken [9].

B. Key Management

Key management is a process that needs to be performed effectively. Whole system is vulnerable if same key pair is used for every machine. Keys can be stolen and there is a need to scale linearly to handle loads of keys. At the same time system can't afford to have weak passphrases as it makes easy target for brute force attacks [11].

Solution: One can secure the key management process from the beginning and by being inconspicuous, automated, and active. This is the only way to ensure that sensitive data is not vulnerable when it is going to the cloud. Additionally, the keys need to be secured mutually, and the process of retrieval should also be very difficult and tedious, to ensure that secured data can never be granted access without a proper authorization [5].

C. Cloud Credentials

The main idea behind cloud is that it provides nearly an unlimited amount of storage for everyone. Usually the enterprise's data is stored alongside the customers' data. This might cause a potential data breach via third parties. This can have severe results - in theory - by the fact that access to the cloud is restricted based on user credentials; although those credentials are also stored on the cloud and is prone to change s remarkably in strength of the security, based on every users' password patterns, meaning that even these credentials are subject to compromise. While a credential, compromise may not be a very big problem or give attackers access to the data within ones files but it could allow them to perform other tasks such as making copies or deleting them [5].

Solution: One can counter this security risk by encrypting all the data, which is vulnerable, and securing the unique credentials, which might require one to invest in a secure service that manages the passwords [5].

D. Malicious Insiders

When a system is attacked by people who are a part of the organization itself it counts as a malicious insider attack. This threat can be posed by the employees, contractors and/or the third party business partners of the organization. This attack leads to loss of user's integrity, confidentiality and security. There are different ways in which insiders can attack because of sophistication about internal structure of an organization's data storage structure. This attack is very hard to defend and almost impossible to find a completion for this attack [7].

Solution: At client's side to ensure confidentiality and integrity strong encryption techniques can be used. Separating duties helps in maintaining a clear boundary so that no unauthorized access is given. Generating and maintaining logs can help in detecting malicious activity sooner. Backup of the system should be taken from time to time if in case an attack happens data is not lost [12].

E. Outside Intruder

When a system is attacked from an external origin it is an outsider attack. The infrastructure provider takes care of the security on which one depends for physical security. An outside attack on the cloud storage can take place and in that case, one must take care of the following objectives: (1) Confidentiality, for secure data transfer and its access, and (2) Audit ability, for preventing outside intruder from accessing sensitive data that is stored on the cloud [7].

Solution: Using intrusion detection and prevention systems along with firewalls helps in reducing the risks. Encryption of data keeps the information on the system safer [13].

F. Bring Your Own Device (BYOD)

The latest security risk of cloud is that employees are now having Bring Your Own Device option. It can be predicted that this trend will stay as it benefits both the employee and the employer. It also comes with major security risks if not handled properly. Stolen, lost or devices that have been misused, suggest that, the vulnerable data of organization is now is not secure anymore. This third party could attack the company's network and steal valuable information. Discovering a data breach on an external (BYOD) system is also more difficult, as it is nearly impossible to track and monitor employee devices without the proper sophisticated tools in place [5].

Solution: Password protected access control along with optimization of user's access control and application permission settings. This helps in controlling what an application can use and ensures no unwanted program's access is given [10].

IV. SUSTAINABLE PROSPECTIVE

Most of the security issues that come with cloud's storage can be minimized with the use of strong cryptographic encryption and key management techniques. Existing cryptographic methods are Advanced Encryption Algorithm (AES), Data Encryption Standard (DES), Triple-DES, Blowfish, International Data Encryption Algorithm (IDEA), Homomorphic Encryption, and Rivest-shamir-Adleman (RSA) [14].

Cryptographic technique RSA is very popular. In RSA we have to select a strongest key pair p and q to generate modulus n. The condition being both p and q must be prime numbers. It provides difficulty to factor n with the use of a specific factoring method (n=p*q). The encryption key (e, n) is known publicly hence, if someone can factor n it is easy to discover d (decryption exponent). So the selection of prime numbers is very important. Otherwise the method used for selecting prime numbers must be efficient. This is the main feature of RSA. The size of RSA key typically refers to the size of n, if p and q are large numbers of the same length then it's very hard to factor the product n. The size of the key depends on the security need. If the size is larger it provides good security but the RSA operation is slower [8].

To increase the security and at the same time increasing the speed, the combination of RSA and Fermat's Little theorem as the cryptographic technique for key exchange can be used [8]. Fermat's little theorem is a fundamental theorem in elementary number theory including primality testing and public-key cryptography. It is helpful for computing powers of integers modulo numbers. One can say that it is a special case of Euler's theorem and is important in applications of elementary number theory [15]. By use of this the reliability of encryption algorithm also increases [8].

V. CONCLUSION

Existing types of cloud services with emphasis on storage of data offered as a service are reviewed. The security issues in present day cloud storage have been elaborated. A cryptographic technique for enhanced security with increased speed is suggested.

VI. REFERENCES

[1] http://searchcloudcomputing.techtarget.com/definition/cloud-computing accessed on: 27 Nov 2017

[2] https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/ accessed on: 30 Nov 2017

[3] https://aws.amazon.com/what-is-cloud-storage/ accessed on: 30 Nov 2017

[4] http://searchstorage.techtarget.com/definition/Storage-as-a-Service-SaaS accessed on: 8 Nov 2017

[5] https://digitalguardian.com/blog/6-security-risks-enterprises-using-cloud-storage-and-file-sharing-apps accessed on: 30 Nov 2017

[6] https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html accessed on 18 Nov 2017

[7] Naresh vurukonda, and B.Thirumala Rao, "A Study on Data Storage Security Issues in Cloud Computing" in 2nd International Conference on Intelligent Computing, Communication & Convergence, ICCC - 2016, Bhubaneswar, Odisha, India

[8] Balkees Mohamed Shereek, ZaitonMuda, and SharifahYasin, "Improve Cloud Computing Security Using RSA Encryption With Fermat's Little Theorem" in IOSR Journal of Engineering, Vol. 04, Issue 02 (February. 2014), ||V6|| PP 01-08

[9] https://securosis.com/blog/cloud-data-security-archive-and-delete-rough-cut accessed on: 06 Dec 2017

[10] https://www.veracode.com/security/byod-security accessed on: 11 Dec 2017

[11] https://www.joyent.com/blog/cloud-security-the-challenges-with-key-management-in-the-cloud-and-everywhere-else accessed on: 11 Dec 2017

[12] Atulay Mahajan, and Sangeeta Sharma, "The Malicious Insiders Threat in the Cloud" in International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April 2015

[13] https://www.sam-solutions.com/blog/top-5-tips-for-cloud-computing-security/ accessed on: 11 Dec 2017

[14] Ashima Pansotra, and Simar Preet Singh, "Cloud Security Algorithms" in International Journal of Security and Its Applications Vol.9, No.10 (2015), pp.353-360

[15] https://brilliant.org/wiki/fermats-little-theorem/ accessed on: 12 Dec 2017