Analysis of Cloud Storage Information Security and It's Various Methods

Priyanka Vishwakarma
Department of Computer Science & Engineering, NIIST
RGPV University
Bhopal, INDIA
priyanka1032@gmail.com

Mahendra Sahare
Professor, Department of Computer Science & Engineering,
NIIST, RGPV University
Bhopal, INDIA
mahendrasahare1110@gmail.com

***Abstract*—** Cloud computing is the latest paradigm in IT field promising trends. It provides the resources similar to accessibility of data, minimum cost and several other uses. But the major issue for cloud is the security of the information which is stored in the cloud. Various methods and specialized techniques are combined together for providing information security to data which is stored in cloud in this paper. The aim of this paper is to analyze various cryptographic techniques and to discuss about various security techniques over cloud and user authentication which is most helpful and useful in the information security over cloud.

Keywords— *Cloud Computing, Availability, Encryption, Decryption, Security, integrity, Confidentiality.*

*****

I. INTRODUCTION

As more and more demands for Information Technology (IT) services rise, here also increasing needs to expand IT architecture and in consequence, IT service providers are faced with challenges of expanding the structures and infrastructures with small expenditure and minimum time in order to provide rising demands from their customers. To address these business challenges and commercial interests, cloud-computing architecture was developed. Cloud computing architecture is an environment of IT resources for particular services which is outsourced to customers [1]. Cloud computing, the cloud service provider is known as cloud provider which is an organization that provides cloud computing service. On the other hand the organization that receives the cloud computing service is known as the cloud customer. Cloud computing is not a novel concept, however it is rising now and it will have major role in the next 10 years or more [1]. It is an increasing concept because of several reasons including reduction in cost and energy consumption of the shared computing resources (servers, software, storage, and networking) [2]. It also enables effective IT resources usage and increases flexibility for expanding new infrastructures in instant time [2]. Like traditional computing environments, cloud computing brings risks and security concerns to the business that need to be considered appropriately. Such risks and security concerns include challenges in handling privileged user access, ensuring legal and regulatory compliance, ensuring data segregation, maintaining data recovery, difficulty in investigating illegal activities, and lack of assurance of long-term viability of the cloud provider [3]. Due to these challenges cloud customers therefore need to institute mechanisms to measure and improve security of their information assets operating in the cloud. Among the alternatives available to the cloud customer for monitoring, measuring and hence improving information security of the assets managed in the cloud is to develop information security metrics.

II. IMPORTANCE OF SECURITY IN CLOUD COMPUTING

The power, flexibility and ease of use of cloud computing comes with lot of security challenges. Even though cloud computing is a new intuitive way to access applications and make work simple, there are a number of challenges/issues that can affect its adoption. this field reveals some issues. They are: Service Level Agreements (SLA), what to migrate, security, etc. [4]. Cloud computing has a feature of automatic updates, which means a single change by an administrator to an application would reflect on all its users. This advertently also leads to the conclusion that any faults in the software are visible to a large number of users immediately, which is a major risk for any organization with little security. It is also agreed up on by many researchers that security is a huge concern for adoption of cloud computing. A survey by IDC on 263 executives also shows that security is ranked first among challenges in cloud computing [5][6]. Even though a company boasts to have top class security and does not update its security policies from time to time, it will be prone to security breaches in near future. In this regard, through this detailed study, we propose to update the readers with different distinctions (types of) in security challenges and their solutions. We also include real-time practices to mitigate challenges, include improved solutions proposed by researchers to show which areas of cloud computing need more attention.

III. SECURITY ISSUES WITH CLOUD COMPUTING

The key benefits with cloud computing are discussed in the previous section and apart from, this, there are some key security issues and they are as discussed below:

3.1 Privacy issues

As all the cloud services are available at the remote locations, users can't have the complete control over their data. But it is always their basic right to protect their data and they have an intension to view all the database operations. Privacy is the main concern to be considered here, and if the cloud services can't provide the level of privacy it can be considered as the main security threat. These privacy issues are mainly irritating across the public clouds, where the access to the clouds is through the public domains.

3.2 Availability and backup

In general most of the client software's and databases are maintained across the remote locations across cloud computing. If the required resources are not available at peak times and even the backup failing across the clouds, this situation definitely leads to lots of security issues.

3.3 Access issues

Cloud computing has the threat of accessing the sensitive information. There are lots of Chances where the information stored across the cloud may be lead to theft by the intruders and hackers.

3.4 Trust

Trust is always required across the cloud computing implementation. A mutual trust between the vendors and the clients is essential and if it is missing the overall security of the cloud is affected a lot.

3.5 Illegal secondary usages

There are lots of chances where the illegal secondary usage of information across clouds may happen. Most of the cloud business models reveal that, service providers can use the user's data for the secondary usage and this may lead to serious security threats

IV. SURVEY OF SECURITY IN CLOUD COMPUTING

A. *Confidentiality*

For both enterprises using cloud environments and cloud service providers, encryption is a critical requirement for securing data. Vormetric encryption provides an uncomplicated means of protection comprising fine-grained access controls key management, and advanced security intelligence data to protect sensitive data-at-rest within public, private, and hybrid cloud environments [7]. Through cloud encryption for cloud implementations, one can meet compliance requirements of access controls for protected data separation of duties, encryption, including PCI- DSS and Data Accross Borders [8]. In addition, cloud encryption can help protect against data breach incidents through the use of policy-based access controls on protected data, key management, and secure encryption in cloud environments as show in Fig1.

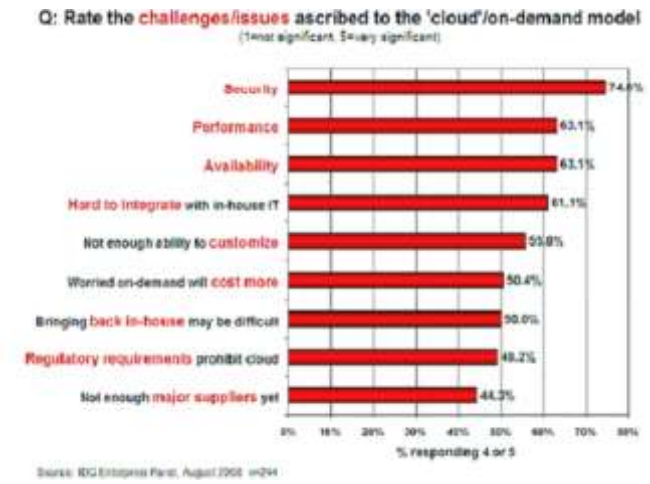

Fig.1. Ratings given to the various challenges/issues ascribed to the "cloud"/on-demand model.

The risks also include those posed by the exposure of customer data to cloud providers and of data exposure because of the shared, comingled data storage used to support cloud environments. Furthermore, cloud computing encryption(s) provides raw security intelligence on data access to encryption protect information; such intelligence enables a Security Information and Event Management (SIEM) solution for recognizing advanced persistent threats or malicious insiders [9].Encryption provides a single, scalable solution that can easily encrypt any file, database, or application wherever they reside on supported operating and file systems, without sacrificing application performance and while avoiding key management complexity. Furthermore, cloud encryption includes seamless key management within the solution and is fully transparent to applications and users, thereby allowing existing processes and usage to continue with no changes [10].

B. *Integrity*

The sequences used in the Transport Layer Security (TLS)/Secure Sockets Layer (SSL) protocol are illustrated in Fig. 2. While the TLS/SSL segments of our proposed framework were being processed, we observed underutilized computation and network resources on both the server and client sides that result from the sporadic computation and communication bottlenecks that occur when the network and computation workloads are varied. When the given network and computation resources are under-utilized, the TLS/SSL

throughput can be improved by maximizing the utilization of the given resources.

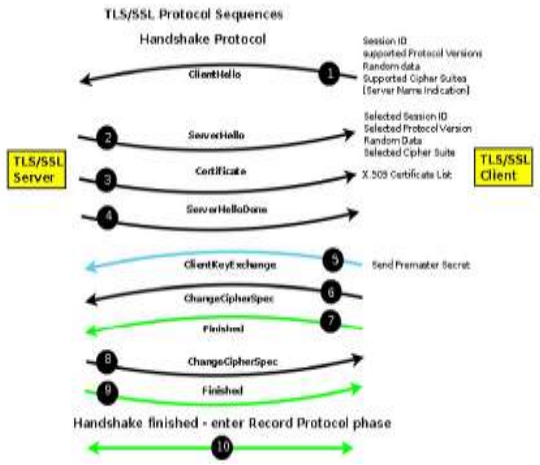

Fig 2: TLS/SSL Protocol Sequence

Applying a specific compression method to a TLS/SSL connection may not be optimal if the connection and computation workload are different and dynamic. If excessive data are loaded for a low-bandwidth TLS/SSL connection, a compression mechanism reflecting environment heterogeneity (such as the device, network, and cloud) should be applied. However, considering that conventional TLS/SSL mechanisms provide a static compression mode, a renegotiation request by an application must alter the compression algorithm to be applied. Therefore, a mechanism that enables TLS/SSL to identify the best compression technique for TLS/SSL connections in a timely and transparent manner must be applied while considering the aspects specified.

C. *Availability*

Business organizations must have "always on" IT solutions because it results in increased costs and can sometimes contribute to a loss of consumer confidence due to interruptions in computing services. Cloud computing fundamentally relies on the Internet. Thus, those companies who are interested in expanding or initiating their work on cloud-based services must know the working of IT consulting firm that can show them how to organize bandwidth levels and meet their IT needs.

1) *Examples of Cloud Failures:* The importance of the availability of cloud resources has been demonstrated by the recent outages of several high-profile cloud providers, with Amazon and Google being among the most notable.

2) *High availability*: However, increasing cloud computing data storage and assuring reliability of data in terms of availability and correctness are very important. While redundancy can be added to data for reliability, this can be a challenging problem in "pay-as-you-use" cloud paradigm, where users always want to efficiently resolve corruption detection and data repair. Prior erasure codes or network coding techniques used in distributed storage systems have either high decoding computational cost for data users or too great a burden for data owners in terms of data repair and being online.

V. RELATED WORK

There are various works which are already done in this field. Some of those are listed below:

- Chao YANG, Weiwei LIN*, Mingqi LIU, in their work entitled "A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security," [11] indicated that the technology of cloud has been expanding in past years because of its power to allow on-demand, elastic, authentic and affordable services to users. With the increased use of cloud application being available, the serious concern is cloud data security.

- Zhen Chen*, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen, in their work entitled "Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System," [12] indicated that Security in the internet is always a challenge along with security concerns such as phishing attacks, spams and internet worms. A well-organized distributed network attacks, Botnets contains large number of bots that generate vast quantity of junk e-mail or launch Distributed Denial of Service (DDoS) attacks on dupe's hosts. They proposed a practical collaborative network security management system with an efficient collaborative Unified Threat Management (UTM) and traffic prober to resolve these problems.

- Huang Jing, LI Renfa, and Tang Zhuo, in their work entitled "The Research of the Data Security for Cloud Disk Based on the Hadoop Framework," [13] indicated that in order to solve the existing security problem such as transmission, storage security problems, etc, of the distributed network cloud disk, a Hadoop based network cloud disk safety storage scheme is proposed. A selective encryption scheme based on the different confidential level of user data, which gives full consideration to the following security issues, such as data transmission in the network, the security of the user, no verification for user data, the user data privacy might be leaked, etc. Combined with identity authentication of RSA and the rapid encryption of symmetric encryption algorithm, the performance of Hadoop and overtime checking, the distributed network cloud data security storage disk can supply effective, secured, and stable effect. Finally BANLOGIC proves the security of the scheme. Aiming at the existing popular cloud disc security weakness, they put forward a security encryption schemes based on Hadoop, which satisfy the data transmission and storage security and satisfy the server executes digital signature for client data at

the same time. It is a distributed encryption system that could reduce the burden on the server, and finally achieve security, stability, and efficient and effective storage. Our current system does not have enough sophistication. In the future versions of our system, they plan to implement a more sophisticated technique for encryption and authentication.

- Said Aminzou, Brahim ER-RAHA, Youness Idrissi Khamlichi, Karim Afdel, Mustapha Machkour, in their work entitled "Towards a Secure Access to Patient Data in Cloud Computing Environments," [14] pointed that in the modern health service, data are stored in a Data Center and only authorized users can access it. However, this Data are prone to be exposed to a number of attacks; especially by the Cloud provider's Personnel with privileged access. To avoid unauthorized access to comprehensive content of data center including patient's information. They propose a content-based watermarking technique. patient and a digest information are encrypted, before being embedded into LSB's bitplane of image associated to the patient. This image is integrated directly into the database. Hadoop system with the integrate functions; HOFS and Map Reduce will play the key roles for our solution. In this paper, they have implemented a security architecture using watermarking and encryption techniques to secure the management of medical image and patient's data in cloud environment. The presented method and architecture will be helpful for enhancing data security in public and private cloud. So, the proposed method will play an important role in the future.

VI. CONCLUSION

By the comparison of base paper with literature survey of several papers, it is concluded that, integrity check, authentication and protection of data are done here and in a cloud computing environment there are many security algorithms which are currently used. Apart from this to increase the security level in the cloud environment there are still there too many areas which require further enhancements like more efficient algorithms can be developed. In future we will suggest efficient encryption algorithm for a cloud environment

REFERENCES

[1] Zaerens, K, "Enabling the Benefits of Cloud Computing in a Military Context," Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, Page(s):166 – 173.

[2] Gibson, J., Athabasca Univ., Athabasca, Rondeau, R., Eveleigh, D., Qing Tan, "Benefits and challenges of three cloud computing service models," Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on IEEE, Page(s):198 – 205.

[3] Yeager, William J. and Morin, Jean-Henry, "Introduction to Secure Cloud Computing Mini track," System Sciences (HICSS), 2013 46th Hawaii International Conference on Date of Conference:7-10 Jan. 2013, Page(s):4957, IEEE.

[4] Hamze, M. and Togni, "Autonomic Brokerage Service for an End-to-End Cloud Networking Service Level Agreement," Network Cloud Computing and Applications (NCCA), 2014 IEEE 3rd Symposium on Date of Conference: 5-7 Feb. 2014, Page(s):54-61.

[5] Whaiduzzaman, M., Gani A., "Measuring security for cloud service provider: A Third Party approach," Electrical Information and Communication Technology (EICT), 2013 International Conference on Date of Conference: 13-15 Feb. 2014, Page(s):1-6.

[6] Hale, M.L, Gamble, R., "SecAgreement: Advancing Security Risk Calculations in Cloud Services," Services (SERVICES), 2012 IEEE Eighth World Congress on Date of Conference:24-29 June 2012, Page(s):133-140.

[7] P. Ayers, "Securing and controlling data in the cloud," Computer Fraud & Security, vol. 2012, no. 11, pp. 16-20, 2012.

[8] S. Subashini, and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.

[9] J. R. Vacca, Computer and information security handbook: Newnes, 2012.

[10] B. Aboba, and P. Eronen, "Extensible authentication protocol (EAP) key management framework," 2008.

[11] Chao YANG, Weiwei LIN*, Mingqi LIU, "A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security," 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies.

[12] Zhen Chen*, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen, "Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System," TSINGHUA SCIENCE AND TECHNOLOGY I S S N 1 0 07 - 0 2 14 0 5 /1 2 p p 4 0-5 0 Volume 18, Number 1, February 2013.

[13] First A. Huang Jing, Second B. LI Renfa, and Third C. Tang Zhuo, "The Research of the Data Security for Cloud Disk Based on the Hadoop Framework," 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, Beijing, China, 978-1-4673-6249-8/13/$31.00 ©2013 IEEE.

[14] Said Aminzou, Brahim ER-RAHA, Youness Idrissi Khamlichi, Karim Afdel, Mustapha Machkour, "Towards a Secure Access to Patient Data in Cloud Computing Environments," 978-14 799. {) 324-5/ 13/$31.00 -20 13 IEEE.