IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-8 E-ISSN: 2347-2693

Data Security and Service Overloading in Cloud Computing -An Overview

Ramesh Prasad Vishwakarma[1*], Sitendra Tamrakar[2], Rishi Kumar Sharma[3]

[1*]Dept. of IT, AISECT University, Bhopal, India
[2]Dept. of CS, AISECT University Bhopal, India
[3]Dept. of CS, AISECT University Bhopal, India

**Corresponding Author: rameshaisect@gmail.com,*

Available online at: www.ijcseonline.org

Received: 12/Jul/2017, Revised: 24/Jul/2017, Accepted: 20/Aug/2017, Published: 30/Aug/2017

***Abstract*—** In the modern time of computing, Cloud computing will perform a major technical role in the IT world. Although various cloud service models are there present, Infrastructure as a Service (IAAS) has become the base of the next future Network of Services (NOS). Several advantages of cloud computing attracts the persons and organization to move their data from remote to the cloud. Cloud Providers mostly focus on providing services and provides a lesser focus on data security and privacy which is the main side of cloud computing. Since the single cloud storage does not fulfill the demands of the individuals and organizations, a move towards multi-cloud storage (MCS) has been emerged. In this report presents an overview of motivation of service overloading, attackers, different techniques and its limitations made to protect data security in the cloud storage .In this paper also explains the usual challenges in cloud storage services. This work delivers a superior solution in the service over loading architecture and key thought in the decision making process for the individuals and organizations in the adoption of superior cloud storage service.

***Keywords*—** Service Overloading, Cloud Security, Data Security, Single and Multi-Cloud Storage.

I. INTRODUCTION

Nowadays, several businesses are budding to start using Cloud Computing (Hayes, 2008) architectures as a new technique of managing cloud data centers, enabling efficient provisioning of virtual IT (VIT) architectures. Such virtual resources service is dynamically created and dismantled on-demand, providing new pay-as-you-go business models for the usage of infrastructures. The cloud computing mechanism is a rental service environment, which implies that a single architecture has several users' applications. Multi-cloud is a blend of multiple clouds like public, private or hybrid clouds, including managed services or service providers. In today's world information storage or sharing means business [1-8].

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 dynamic to the cloud is to detract the costs .In cloud computing, security may be assured of data which have to be stored in cloud storage. Through data sharing, higher productivity levels are achieved.

Privacy protection and data integrity are two of the major grave security issues related to the user data. But in the case of cloud computing, the data is saved on an autonomous business party that contributes data storage as a subscription service. The users have to trust the CSP (cloud service provider) with integrity of their data [1,2,3, 9-14].While data 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 any level. It is absolutely vital, that in today's world, one must have certainty that secrets, whether they are composed of personal data or information of national importance, remain secret as they pass through several elements encountered along the communication path from source to destination.

The logical access path of each file slices is changing dynamically with respect to time. It protects the user data from unauthorized users, since the logical path is changed; the intruders cannot able to retrieve valid data. Storage services based on public clouds such as Rackspace and Amazon's S3 provide customers with scalable and dynamic storage.

First, the enterprise should trust the cloud provider. Second, the enterprise should ascertain that its clients have enough reason to trust an equivalent provider [2,3,6,15-19]. In the public clouds, all of the three main common cloud service (IaaS, PaaS, SaaS) shares the commonality that the end-cloud users' digital assets are taken from an intra-organizational to an inter-organizational context. This creates a number of

difficulties, among which security facets are regarded as the most censorious factors when considering cloud computing adoption [3,16, 20,21,22,23].

Any info related to the database in which one specific column or attribute is to be secured. In order to store the data securely, many cryptographic techniques and system are available. On the other hand files or information are the unstructured data in several formats which easily exist in adopting the cloud storage service. Nearly all the cloud storage service providers are maintaining a secure infrastructure to store all types of file formats. By bad luck, many storage service providers provide focus on security to support all types of data or file formats and in their architectures.

Most of the service providers will guarantee 99.9% security is possible with (SLA) Service Level Agreement, but no one of the provider has an integrated tool or framework to self detect those challenges. The data and file security plays a main role in the cloud storage system. As aforesaid many file formats are available in many sizes, it's not an easy task for a cloud service provider (CSP) to give protection or provision to upload for all data formats. Some of the file formats, particularly video files may not supported by the provider's framework or security tools. There are three main reasons that makes cloud provider to do so. They are size, internet traffic and cost. In [4] hhe makeup of internet traffic itself is changing. Historically, File Transfer Protocol, Hyper Text Transfer Protocol (HTTP) and peer to peer traffic are now available. Today video is already dominating the mix and by 2020, it is projected that video will signify more than 98 percent of all user 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.

Service, overloading is a concept of service oriented network (SON) that allows DataCenter to define two or more services with the same service name and in the same network. Each service has a unique signature (or header), which is derived from: service / service ID name.

II. RELATED WORK

Privacy preservation and data integrity are two of the major critical security issues related to user data. In conventional paradigm, the organizations had the physical possession of their data, and thus have an ease of implementing preferable data security policies. But in the case of cloud computing, the data is saved on an autonomous business party that contributes data storage as a subscription service. The users have to trust the cloud service provider with integrity of their data. In [1], examined the criticality of the privacy issues in cloud computing, and pointed out that acquiring information from a third party is much easier than from the creator himself.

To provide users with higher and truthful chances to avail proficient security services for their cloud storage at reasonable costs, our model distributes the data units among more than one service provider, in such a route that no one of the SPs can retrieve any meaningful information from the pieces of data stored on its servers, without getting some lot of pieces of data from alternative service providers. Therefore, the traditional one service provider based cryptographic systems does not seem too much promising. In [5,9,11,21], well-read distributing the data over multiple clouds or networks in such a route that if an adversary is able to intrude in one network, still he cannot retrieve any weighty data, because its complementary pieces are stored in the other network. Our approach is similar to this technique, because both aim to remove the centralized distribution of cloud data. This is why in our model; we propose to use a distributed approach, in which all the pieces of the data are required out of the entire distribution range, for well-turned retrieval.

III. CLOUD SECURITY ISSUES

Cloud security includes PC, Network security, and major, part of completely data security. It means a large set of policies and controls sent to secure data and file, applications, and the associated infrastructure of cloud computing. For any organization, secure data are increasingly valued for being really a record that serves as a magnificent confirmation of outness.

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; [6] in 2014, Harvard Business Review uncovers that different 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. This means that control management is regularly defective and security experts frequently leave dangerous data, data associated with legal or harmony commands, and few 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.

IV. THREATS

There are a number of types of privacy and security threats in the cloud. The following describes the outline of

varied threats in cloud computing and their impact on the 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 weaknesses or bad security practices. Corporate Network and Telecom operator organization gets affected by this attack. These attacks can be minimized by executing a multifactor authentication and encryption.
b) Insufficient Identity, Credential and Access Management: This attack is caused due to the absence of identity verification, lack of examining 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 power full attack. Any organization that has weaknesses in data flows and architecture or system design in the development life cycle. Security-specific code reviews and hard 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 organizations like 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 the technical team.
e) Account Hijacking: Account or any service hijacking is not new work. Attack strategies like fraud ,phishing and exploitation of software package weaknesses still reach results. If an attacker avails access to your identifications, they will listen in on your activities and transactions, change information, come falsified info and direct your customers to illegal sites.
f) Malicious Insiders: A malicious insider risk to an association is any employee, contractual worker, or different business partner who has or had approved access to an organization's network. A malevolent insider, such as a cloud service administrator, can access potentially sensitive information. Cloud Service providers have a huge impact on this attack. 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 logical property. Any one organization who user unsecure networks can get easily affected by this attack. Consciousness programs that are regularly reinforced.
h) Data Loss: Data stored within the cloud will be lost for reasons aside from malevolent attacks. An accidental deletion by the cloud service provider, or worse, a physical devastation like a fireplace or an earthquake, will cause the permanent loss of client knowledge. Any organization such as health and banking care are highly targeted for this type of attack. Adequate measures to back up data and data information, following best exercises 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 take cloud computing technologies and opt for CSPs while not performing due diligence exposes itself to a innumerable of business, technical, legal and adherence risks. Any one organization that has not studied the adherence of new heritage 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 legal service users confused and angry about why the service isn't answering. Cloud Service Providers (CSP) and private Data centers can be affected by this attack. Auto Detection or monitoring tool is required when a website becomes slow. This work describes the overview of Multi-Cloud storage approaches which explains the techniques, challenges and its limitations. Many similar approaches have 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 fulfill their demands.

V. SERVICE OVERLOADING

If any clouds have multiple services with same names but different parameters time (PT) then they are said to be overloaded. Service, overloading allows you to use the same service name for a different range, to perform, either same or different service in the same cloud network.

Service overloading is usually used to enhance the readability of the cloud security. If you have to perform single operation, but with different number or types of user, then you can simply service overload the cloud.

"Overloading is the reuse of the same service name or network for two or more distinct user or operations". Service overloading is the general concept of service oriented network .A service can be declared more than once with different operations. This service is called overloading. It is the Data Center job which one is the right to choose. If it cloud service provider sense to you then I should say that one service name for different operations have the advantage of good readability of a cloud.

VI. CONCLUSION

This work describes the overview of Cloud service overloading approaches and cloud security which explains the techniques, challenges and its limitations. Many similar approaches have been proposed, but there is a shortage of improvement in technical approach. In real time it is a tedious process for individuals, and service providers to fulfill their requirements.

REFERENCES

[1]. Bincy Paul and M. Azath, "*Survey on Preserving Data Privacy in Cloud*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.12, pp.57-61, 2014.

[2]. B. Michael, "*In Cloud Shall We Trust?*"' IEEE Security& Privacy, Sept./Oct. 2009, p. 3.

[3]. F. Gens, "*IT Cloud Services User Survey, pt.2: Top Benefits & Challenges*,"' blog, http://blogs.idc.com /ie/?p=21 0, 2008.

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

[5].P. F. Oliveira, L. Lima, T. T. V. Vinhoza, 1. Barros, M. M'edard, "*Trusted storage over untrusted networks*", IEEE GLOBECOM , Miami, FL.USA, 2010

[6].www.hbr.org

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

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

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

[10] P. Ranjima, Sumathi. D , M. Mathew, P. Sivaprakash, "*Secure Cloud Storage with Access Control: A Survey*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.8, pp.124-126, 2014.

[11]. WANG Liang-Liang, CHEN Ke-Fei, MAO Xian-ping, WANG Yong- Tao, "*Efficient and Provably-Secure Certificateless Proxy Re-encryption Scheme for Secure Cloud Data Sharing*" Journal of Shanghai Jiaotong University, Vol.19, Issue.4, pp.398-405, 2014.

[12]. 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.

[13]. 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) IEEE Twelfth International Symposium, pp.205-210, 2015.

[14].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.

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

[16]. Xu, L., Wu, X., & Zhang, X., "*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, 2012.

[17]. Michael O. Rabin, "*Efficient Dispersal of Information Security, Load Balancing, and Fault Tolerance*", *Journal of Association for Computing Machinery*, pp.335-348, 1989.

[18] P. Thakkar, H.K. Mishra, Z. Shaikh, D. Sharma, "*Image Encryption and Decryption System Using AES for Secure Transmission*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.5, pp.109-114, 2017.

[19]. V.P.Muthukumar and R.Saranya, "*A Survey on Security Threats and Attacks in Cloud Computing*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.11, pp.120-125, 2014.

[20]. J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "*Security and Privacy-Enhancing Multicloud Architectures*," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 212–224, Jul. 2013.

[21]. Nitesh Jain, Pradeep Sharma, "*A Security Key Management Model for Cloud Environment*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.1, pp.45-48, 2017.

[22]. N. Deshai, P. Penchala Swamy, G.P. Saradhi Varma, "*Enhanced Query Processing Technique Using RASP Effective Services in Cloud*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.4, pp.75-77, 2017.

[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, Vol.2, Issue.4, 2015.

