ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

An Overview of Security Challenges in Cloud Computing

Bhuvaneshwaran.S, Balamurugan.K, Dr.Vijayaraj.M

Abstract*— Cloud computing brought flexibility, scalability, and capital cost savings to the IT industry. As more companies turn to cloud solutions, securing cloud based services becomes increasingly important, because for many organizations, the final barrier to adopting cloud computing is whether it is sufficiently secure. More users rely on cloud storage as it is mainly because cloud storage is available to be used by multiple devices (e.g. smart phones, tablets, notebooks, etc.) at the same time. These services often offer adequate protection to user's private data. However, there were cases where user's private data was accessible to other users, since this data is stored in a multi-tenant environment. These incidents reduce the trust of cloud storage service providers, hence there is a need to securely migrate data from one cloud storage provider to another. This paper proposes a design of a service for providing Security as a Service for cloud brokers in a federated cloud. This scheme allows customers to securely migrate from one provider to another. To enable the design of this scheme, possible security and privacy risks of a cloud storage service were analyzed and identified. Moreover, in order to successfully protect private data, data protection requirements (for data retention, sanitization, and processing) were analyzed. The proposed service scheme utilizes various encryption techniques and also includes identity and key management mechanisms, such as federated identity management". While our proposed design meets most of the defined security and privacy requirements, it is still unknown how to properly handle data sanitization, to meet data protection requirements, and provide users data recovery capabilities (backups, versioning, etc.).

Index Terms— **Data Integrity, Dependable Distributed Storage, Cloud Computing.**

I. INTRODUCTION

Cloud computing is not a completely new computing model. The concept has been adapted from the earlier grid computing paradigm, and other distributed systems such as utility computing and cluster computing. In September 2011, the definition and specifications of cloud computing were standardized by the U.S. National Institute of Standards and Technology (NIST). The definition of Cloud Computing introduced by the NIST is Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of positive essential characteristics, three service models, and four deployment models. Cloud computing is available in three different offerings: cloud computing, cloud storage, and Anything as a Service (XaaS).

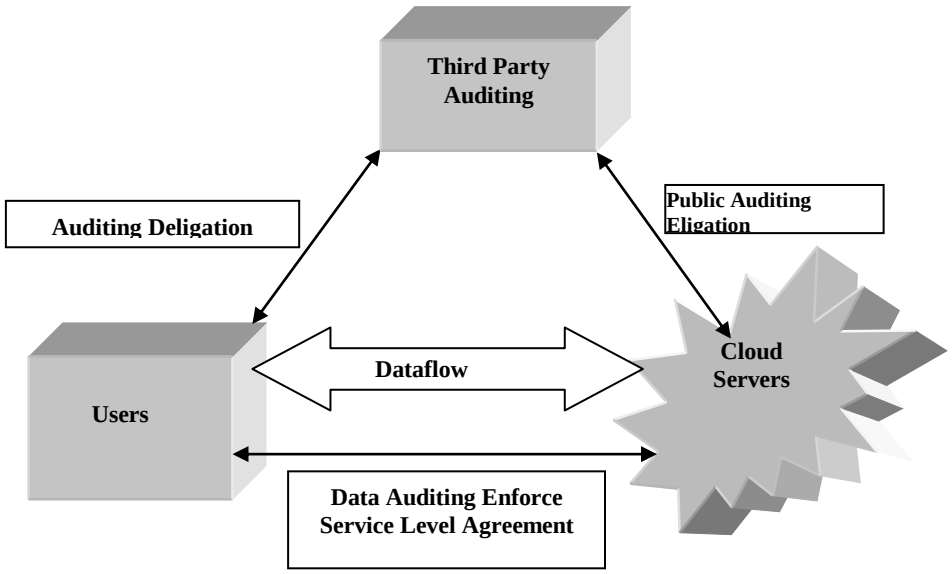

Fig 1: Cloud operation

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

A number of characteristics define cloud data, applications services and infrastructure: Shared resources, software and information, provided to computers and other devices on demand Like the Electricity Grid.

II. RELATED WORK

The word "data" is plural, not singular. The subscript for the permeability of vacuum μ_0 is zero, not a lowercase letter "o." The term for residual magnetization is "remanence"; the adjective is "remanent"; do not write "remnance" or "remnant." Use the word "micrometer" instead of "micron." A graph within a graph is an "inset," not an "insert." The word "alternatively" is preferred to the word "alternately" (unless you really mean something that alternates). Use the word "whereas" instead of "while" (unless you are referring to simultaneous events). Do not use the word "essentially" to mean "approximately" or "effectively." Do not use the word "issue" as a euphemism for "problem." When compositions are not specified, separate chemical symbols by en-dashes; for example, "NiMn" indicates the intermetallic compound $Ni_{0.5}Mn_{0.5}$ whereas "Ni–Mn" indicates an alloy of some composition Ni_xMn_{1-x}.Be aware of the different meanings of the homophones "affect" (usually a verb) and "effect" (usually a noun), "complement" and "compliment," "discreet" and "discrete," "principal" (e.g., "principal investigator") and "principle" (e.g., "principle of measurement"). Do not confuse "imply" and "infer." Prefixes such as "non," "sub," "micro," "multi," and ""ultra" are not independent words; they should be joined to the words they modify, usually without a hyphen. There is no period after the "et" in the Latin abbreviation "et al." (it is also italicized). The abbreviation "i.e.," means "that is," and the abbreviation "e.g.," means "for example" (these abbreviations are not italicized).An excellent style manual and source of information for science writers.

The Cloud Security Alliance (CSA) in has done a great job defining Security as a Service. The European Network and Information Security Agency (ENISA) in described the benefits and risks of cloud computing. Cloud storage services, such as SpiderOak, introduced a zero knowledge approach which was used in the thesis. In Educause clearly described a federated identity management concept. In Basescu et al. proposed a generic security management framework allowing providers of cloud data management systems to define and enforce complex security policies. In Chow et al. addressed the problem of building a secure cloud storage system which supports dynamic users and data provenance. In Yang and Zhang proposed a generic scheme to enable grained data sharing over the cloud, which does not require key-redistribution and data re-encryption.

In securing cloud data storage service V Y TAUTAS ZAPOL S KAS says Cloud Storage data protection risks. Customers who store their data in a cloud should be familiar with the risks of data being collocated in a shared environment. NIST defines the main data protection risks for stored data in a CSP and the risks when migrating data between providers.

1. Data concentration

Currently, information has a huge value and that data is consolidated into a huge cloud-based data storing facility. Because this data has such high value and it is all in one place it is a clear target for an attack. The basic reasons for such data being desirable target is due to the economy of scale - as a successful attack has a greater yield for the effort of carrying out the attack. As a result an attacker is more interested in exploiting a system which has a lot of data, even though a successful attack may require more effort than an attack against a target that has
Little data and requires slightly less effort.

2. Cloud Storage Security and Privacy Risks

Such information storage vaults require sophisticated security measures including proper password reset operations. As stated in a famous social networking site Twitter was exploited because the site's administrator's account password was reset by someone who successfully answered the security questions. The correct answers were gathered by social engineering. A similar weakness was found in Amazon's Grid Computing Services. An attacker who controls a mail service can access a tremendous number of user accounts as frequently lost passwords for cloud services can be reset by using a Uniform Resource Locator (URL) or code word sent via electronic mail. If an attacker eavesdrops the communication link through which a password reset mail is sent, He or she may electively take over that account.

3. Data isolation

In cloud storage data can take many forms, for instance it can be a container of data or simply a set of _les and associated metadata. In addition, part of a customer's data might be stored within a database (for example, private data such as name, address, and payment card number, etc.). To successfully secure data from unauthorized access, a suitable access control mechanism should be used. Identity management is one of the biggest issues in cloud storage as physical authentication is not possible; hence it is easier in the Internet to impersonate another person than in a reality. Currently data centers other high-level physical security However, there is always a possibility that

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

a rogue employee steals or alters data. Encryption should be used to protect the data, with the encryption keys stored outside of the data center, preferably held by an key escrow service. However, Bruce Schneider has stated in `A variety of \key recovery," \key escrow," and \trusted third party" encryption requirements have been suggested in recent years by government agencies seeking to conduct covert surveillance within the changing environments brought about by new technologies so that these government agencies may continue to conduct covert surveillance. In Jansen and Grance say \Data must be secured while at rest, in transit, and in use, and access to the data must be controlled". Data transfers have been secured by introducing standardized security protocols such as SSL and Transport Layer Security (TLS) However, protection for data at rest has not been standardized yet .

4. Data Sanitization

Data stored in a cloud should be deleted with great care, as forensic tools can be used by both criminals and law enforcement authorities in order to restore deleted data - even in a multi-user environment. Since customers of a cloud storage service share the same storage media, there is a possibility that a cloud storage user can restore other customers' data from a given container. Moreover, it is easy for a rogue employee to recover insecurely deleted customer data.

III. PROBLEM STATEMENT

A. System Model

Representative network architecture for cloud storage service architecture is illustrated in Fig. 1. Three different network entities can be identified as follows:.

User**:** An entity, who has data to be stored in the cloud and relies on the cloud for data storage and computation, can be either enterprise or individual customers.

Cloud Server **(**CS**):** an entity, which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter).

Third-Party Auditor**:** an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated, and distributed manner. Data redundancy can be employed with a technique of erasure correcting code to further tolerate faults or server crash as user's data grow in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations we are considering are block update, delete, insert, and append. Note that in this paper, we put more focus on the support of file-oriented cloud applications other than non file application data, such as social networking data. In other words ,the cloud data we are considering is not expected to be rapidly changing in a relative short period. As users no longer possess their data locally, it is of critical importance to ensure users that their data are being correctly stored and maintained. That is, users should be equipped with security means so that they can make continuous correctness assurance (to enforce cloud storage service-level agreement) of their stored data even without the existence of local copies. In case that users do not necessarily have the time, feasibility or resources to monitor their data online, they can delegate the data auditing tasks to an optional trusted TPA of their respective choices. However, to securely introduce such a TPA, any possible leakage of user's outsourced data toward TPA through the auditing protocol should be prohibited. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead. These authentication handshakes are omitted.

IV. DATA PROTECTION REQUIREMENTS

Where it was possible to recover data from hard drives that had been disposed of by selling them on the Ebay Online Store. Kissel, et al [10]. Provide guidelines on how data storage should be properly sanitized. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization applies to repurposed equipment (usually after hardware upgrade), backup copies, and also to any data which is in storage after the end of the contract.

A.Digital Trust in the Cloud Says about Cloud Trust Protocol:

Cloud Trust Protocol (CTP): The Cloud Trust Protocol (CTP) is the mechanism by which cloud service consumers (also known as "cloud users" or "cloud service owners") ask for and receive information about the elements of transparency as applied to cloud service providers. The primary purpose of the CTP and the elements of

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

transparency is to generate evidence-based confidence that everything that is claimed to be happening in the cloud is indeed happening as described, and nothing else. This is a classic application of the definition of digital trust.4 and, assured of such evidence, cloud consumers become liberated to bring more sensitive and valuable business functions to the cloud, and reap even larger payoffs. With the CTP cloud consumers are provided a way to find out important pieces of information concerning the compliance, security, privacy, integrity, and operational security history of service elements being performed "in the cloud". These important pieces of information are known as the "elements of transparency", and they deliver testimony about essential security configuration and operational characteristics for systems deployed in the cloud. The elements of transparency empower the cloud consumer with the right information to make the right choices about what processing and data to put in the cloud or leave in the cloud, and to decide which cloud is best suited to satisfy processing needs. This is the nature of digital trust, and reinforces again why such reclaimed transparency is so essential to new enterprise value creation. Transparency of certain important elements of information is at the root of digital trust, and thus the source of value capture and payoff.

V. FUTURE WORK

To ensure the security and dependability for cloud data storage under the aforementioned adversary model, we aim to design efficient mechanisms for dynamic data verification and operation and achieve the following goals:

1**.** Storage correctness**:** to ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.

2. Fast localization of data error: to effectively locate the malfunctioning server when data corruption has been detected.

3. Dynamic data support: to maintain the same level of storage correctness assurance even if users modify, Delete, or append their data files in the cloud.

4. Dependability**:** to enhance data availability against Byzantine failures, malicious data modification and Server colluding attacks, i.e., minimizing the effect brought by data errors or server failures.

5. Lightweight**:** to enable users to perform storage correctness checks with minimum overhead.

VI. CONCLUSION

The data storage security is the issue here. We have to find a new privacy mechanism which is used to resolve this issue.

REFERENCES

[1] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.

[2] N.Gohring, "Amazon's S3 down for several hours," Online at http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html, 2008.

[3] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS '07, pp. 584–597, 2007.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc.of Asiacrypt '08, Dec. 2008.

[5] K. D. Bowers, A. Juels, and A. Opera, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 008/175, 2008, http://eprint.iacr.org/.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data ossession at Untrusted Stores," Proc. ofCCS '07, pp. 598–609, 2007.

[7] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. of SecureComm '08, pp. 1–10, 2008.

[8] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. of ICDCS '06, pp. 12–12, 2006.

[9] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," Proc. of the 2003 USENIX Annual Technical Conference (General Track), pp. 29–41, 2003.

[10] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report 2008/489, 2008, http://eprint.iacr.org/.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

[11] L. Carter and M. Wegman, "Universal Hash Functions," Journal of Computer and System Sciences, vol. 18, no. 2, pp. 143–154, 1979.

[12] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasure coded Data," Proc. 26th ACM Symposium on Principles of Distributed Computing, pp. 139–146, 2007.

[13] J. S. Plank and Y. Ding, "Note: Correction to the 1997 Tutorial on Reed-Solomon Coding," University of Tennessee, Tech. Rep. CS-03- 504, 2003.

[14] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," Proc. of IEEE INFOCOM, 2009.

[15] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," Proc. of ICDCS '08, pp. 411–420, 2008.

[16] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and Untreatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.

[17] M. A. Shah, M. Baker, J. C. Mogul, and R. Swami Nathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop on Hot Topics in Operating Systems (HOTOS '07), pp. 1–6, 2007.

AUTHOR BIOGRAPHY

Bhuvaneshwaran.S received his B.E degree from ANNA University, Chennai in 2010.Currently he is pursuing his Masters degree in Engineering at Einstein College of Engineering, Tirunelveli, Tamilnadu, India

Balamurugan.K received his B.E degree from Manonmanium Sundaranar University, Tamilnadu, India during 2002 and M.E degree from Anna University Chennai during 2005. Currently he is pursuing PhD programme in the area of Network-on-chip (NOC) at Anna University Chennai. He is working as Assistant professor in the Department of Electronics and Communication Engineering at Einstein College of Engineering, Tirunelveli, and Tamilnadu. He has published his research papers in various National and International Conferences and Journals in the field of VLSI Design.

Dr.Vijayaraj received his B.E degree from Madras University, Tamilnadu, and India M.E degree from Madurai Kamaraj University Madurai and Doctoral degree from Anna University Chennai. He has 25 years of teaching and research experience in the field of Wireless Communication. Currently he is working as Associate Professor in the Department of Electronics and Communication Engineering at Government College of Engineering, Tirunelveli, and Tamilnadu. He has published his research papers in various National and International Conferences and Journals in the field of VLSI Design.