ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Establishment of Increased Security for Data Storage in Cloud Computing

Madhuri Mamidisetti
Persuing M.Tech,
Department of CSE,
B.V.Raju Institute of Technology,
Vishnupur, Narsapur, Medak Dt. Telengana, India.

J.Suman, M.Tech
Assistant Professor,
Department of CSE,
B.V.Raju Institute of Technology,
Vishnupur, Narsapur, Medak Dt. Telengana, India.

Abstract:

Cloud Computing is one of the best choice for Small and Medium Sized Entrepreneurs' in the world. This has been used widely to cater the needs of organizations with different software applications through SAAS operations of cloud. Cloud has gifted the organizations the platform as a service at most economical rates. The economical rates and swift services has given rise to the cloud computing fame. But the recent privacy issues and security challenges have degraded the cloud computing marketing. North Bridge (2013).The proposed paper is focusing on privacy preservation using third party auditor for cloud computing data storage. In this model a Third Party Auditor will be incorporated to audit efficiently the cloud data storage without acquiring the local copy of data and without keeping any online burden to the cloud computing user.

Key words:

Cloud Computing, Data security, Privacy Preserving Model, Third Party Auditor, Cloud Storage.

Introduction:

Cloud market has fallen down because of the data storage security problems, quality of services and privacy preserving issues in cloud computing. The research scholars have done enough research to admeasure the problems but still lot of loop holes and missing links are notified in cloud computing to arrest the problems. There is a great need to revive the situation by doing the research work to ensure data storage security in cloud computing. There are many research works tried to ensure the data security in cloud computing servers with different techniques like digital encryption, fuzzy key word search etc.

The ultimate solution for data security and data storages should be given to arrest the problems due to Byzantine failure, malicious data modification attack and server colluding attacks. Ricardo Puttini (2013) For this reason, the proposed project looks at developing a cloud based patient record system involving encryption and decryption and to allow authorized users to access unencrypted data on an online-patient record system. Content sharing from cloud computing is predominant.

To demonstrate a well secured and privacy preserving content sharing is essentially required in cloud computing and distributed data systems. Encrypting a specific data and storing will hide the data in the database. Decrypting the data and demonstrate the same to the user is also practiced in cloud computing...

Background:

Content sharing from cloud computing is predominant. To demonstrate a well secured and privacy preserving content sharing is essentially required in cloud computing and distributed data systems. Encrypting a specific data and storing will hide the data in the database. Decrypting the data and demonstrate the same to the user is also practiced in cloud computing. But it has not effectively used for data sharing scenarios.

To demonstrate the effective data sharing mechanism for the distinct users without disturbing privacy has to be achieved. To achieve the same an anonymous ID assignment system is identified and implemented in the cloud computing data which has to be demonstrated to the specific users. The system should send the anonymous ID to the distinct users to read the specific data which has been hidden by the owner of the data.

Existing System:

Though Cloud computing is enriched with the special features like agile, reliable, cost effective and measurable delivery of data. Cloud computing has excellent delivery models with identification, Authentication, Authorization, Confidentiality, Integrity, Non-repudiation and availability as information security requirements. it is blamed by the provision of untrustworthy servers located at remote and un-known locations. This feature has become an issue to store sensitive data and confidential data at untrusted servers at unknown remote locations and caused the heavy computation overhead.

Frequently the cloud computing has encountered the security issues such as SQL Injection Attacks, Cross Site Scripting Attacks, Man in the Middle Attacks, Network Level Security Issues, DNS attacks, Sniffer Attacks, BGP Prefix Hijacking and issue of reused IP Address. Apart from these attacks Application level security issues with security concerns with the Hypervisor, Denial of Service Attacks, Cookie Poisoning, Hidden Field Manipulation. Captcha Breaking, Google Hacking and Distributed DOS Attacks are traced in cloud computing.

Drawbacks in Existing system:

The non-technical cyber security threats are regarded as Insider attacks, Poor passwords, Physical Security, Insufficient backup and recovery, improper destruction, Social Engineering and social media. PTAC has successfully inculcate the mitigation for all above mentioned threats and suggested the students to follow consistent implementation of the security plan drastically eradicate the cyber threats and establish the security. – PTAC – IB [2011].

Man-in-Middle Cryptographic Attacks:

MiM attack is carried out when an attacker places himself between two users. Anywhere attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications. - Xu Huang [2010]. Jonathan added demonstrating a cryptographic protocol for security is one of the important tasks in application development. Man-in-the-middle attack modifies the data transmitted from sender to receiver. Xu Huang [2010].

Denial of Service (DoS) Attacks:

QijunGu [2010] says Some of the security professionals have been arguing that cloud has more problems from DoS attacks, because cloud is shared by many users, which makes DoS attacks much more insecure. - QijunGu [2010] A malicious party barrages a server with so many requests that it can't keep up, or cause it to reset in case of Denial of service attack.

AuthenticationAttacks:

Michael Gregg (2010) described the authentication is frequently attacked because it is a weak point in hosting and virtual services. there are some ways to authenticate users, for Example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

The proposed Project:

The present project is designed and developed with Homomorphic encryption, generalization, cryptographic methodology and user access right with special ID allocation. The project is designed and developed to demonstrate the cloud computing environment with Cloud Service Provider, Cloud Consumer and Cloud User access rights. The application is developed to demonstrate the data sharing techniques without any collections, leakage and privacy issues and challenges. The cloud consumer is the data owner and stores the data in the cloud data centers. The location of the data centers are not known to the cloud consumers. The data will be accessed by the customers of the cloud consumers. The customers can be termed as cloud users. The cloud users are allocated with a specific ID which can be changed time to time. Using this ID, the users will access the database of the cloud computers and safely retrieve the data without effecting the others privacy preserving policies. To perform the activity the database creation and maintenance is given to a third party cloud Service.

What is new in this project?

- Designing and developing a third party auditing system for the data storage in cloud servers is predominantly new in this project.

- To handle multiple auditing tasks of cloud users in meticulous way and arrest malicious data and vulnerabilities intruding along with the data insertions.
- Third party auditing system should audit the proof from the cloud server.
- A mechanism which can be run by the server should check the data storage correctness.
- The third party auditing system is enriched with the mechanism to verify the metadata, signatures and MAC address of the data storage.

Modules of the Project:

1. Cloud Consumer
2. TPA
3. Cloud user

Cloud Consumers [data owner]:

Cloud consumer will hive the cloud server from the Cloud Service provider. The cloud consumer will store the data in the cloud servers. The cloud consumer will create cloud users, The data stored by the cloud consumers will be under security and will be accessed by the secured users only.

Third Party Auditing:

Third party auditing system is one security mechanism to store the data into the cloud servers. Third party auditing system is arranged by the cloud consumers as well as the cloud service providers. The cloud service providers would safe guard the server with the help of Third party auditing. Third party auditing will scan the data whatever stored by the cloud consumer then it will decide whether the data can be stored in the server or not. If the data consists of malicious data then the TPA will delete the data from the server. Predominantly the data storage will be audited by the TPA system and allow the data to place in the server. It can be accessed by the authorized user of the Cloud Consumers.

Cloud User [Authorized]:

Cloud users are created by the Cloud consumers. These users are authorized and authenticated users of the cloud consumers.The permitted users only can access the data stored by the Cloud consumers.

The Functionality of the Project:

The project is designed and developed to demonstrate the cloud computing data storage security with the help of Third Party Auditing system. The cloud computing is declining with the security loopholes. These loop holes of security system can be arrested by employing the third party auditing system. The cloud computer is occupied by the cloud consumers. Sometimes the cloud servers are losing the data integrity and confidentiality because of the cloud consumer’s data stealing mechanism. The data stored by the cloud consumers should be streamlined by employing a third party auditor who is most amicable and trustworthy for cloud consumers as well as cloud service providers.

The cloud consumer’s data should be scanned and verified by the Third Party Auditor, then it should be stored in the cloud servers. This data streamlining mechanism will avoid the malicious data storage in the cloud computing servers. When the data is accessed by the cloud users who are created and permitted by the consumers should also approved by the third party auditor. In this present project the Third Party Auditing system will keep an eye on the data accessing items and keeps the track of them. In this way the data storage mechanism will be audited by the Third Party auditor and safely enable the cloud consumer to store the data into the cloud servers.

Encryption: To provide the data security the digital encryption methods are one of the best suited solutions in cloud computing. The data storage should be done with the help of encryption methods and should be accessed by using the specific key supplied to the distinct users. Different encryption methods can be incorporated to safeguard the security of data in cloud computing in respect of data variation and importance. The Digital Encryption standards, Advanced Encryption Standards and Triple DES methods are popular and predominant in cloud computing security incorporation. In the cloud computing to provide highest data security the encryption standards are used with anonymous ID generation to the specific users to access the original content of the stored data.

Project filtered successfully the following threats and attacks:

I.Privacy preserving issues: Cloud computing is facilitating software services to innumerable clients in the world.

At this juncture the same software application consumers are storing the data into the same data center of clouds. The data leakage is identified in the cloud servers. The data of one customer has been revealed to the other customers. This situation has degraded the popularity of the cloud computing growth.

II.Security issues: Cloud computing is working on predominant mechanism. This is virtualization. This mechanism is used to provide data availability and data integrity. But the activities of intruders and hackers have tactically inserting the malicious data into the cloud servers and capturing the valuable data others. This malicious activities have broken the security system of cloud computing. This has to be addressed immediately.

III.Data Collision: The increased number of cloud consumers has loaded the data in the huge cloud servers. The huge amount of data storage from every cloud consumer has given a path to data collision. This situation has also provided the way to capture the data of others at huge amount by the eavesdroppers.

IV.Data Availability: Cloud computing is providing the data integrity and availability to the cloud consumers. This has been utilized by the hackers and intruders to access the data in malicious ways by using pseudo code and authorization methods. The data accessing methods are not so strong in cloud computing to authorize the user with the attributes of identity. The sensitive data from the cloud computing has been eavesdropped by hackers many a time sofar. This issues have to be addressed immediately.

V.Trust: Trust is one of the most important issues faced by the cloud computing. The cloud computing service provider and cloud consumers should have trust in protecting the data from inside attackers and intruders. The service level agreements are not properly formulated so far. The SLAs to protect the cloud computing consumers should be incorporated in times of any data loss or data leakage is taken place.

Conclusion:

The present project is a simulation project to replicate the cloud computing architecture. The project is developed in visual studio and a database is developed with SQL Server.

The present project has successfully demonstrated the functionality of the cloud consumers to store the data in the cloud computing and the third party auditor is incorporated to check the data stored by the cloud consumer. If the data is affected with any malicious code then the third party auditor is rejecting the data to store in cloud computing storage. Similarly the authorised user of cloud can be permitted to access the stored data by the cloud consumer. The data security is aptly followed in this project. The testing of data with malicious code is rejected by the auditor successfully and the data without malicious code is accepted and sent to cloud computing storage point.

References:

[1]Peter Mell, Timothy Grance [2011]The NIST Definition of Cloud Computing - published in NIST Special Publication 800-145.

[2]The Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing

[3]Kuyoro S. O., Ibikunle F. &Awodele O. [2011]International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011 247 Cloud Computing Security Issues and Challenges published in International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011.

[4]Fabio Marturana [2013]Cloud Computing Implications to Digital Forensics

[5]Daniel Ayers [2009]A second generation computer forensic analysis system digital investigation 6 (2009) S34–S42 doi:10.1016/j.diin.2009.06.013

[6]Mrs P.R.LakshmiEswari [2011]Security in Cloud Computing

[7]Jerry Archer from Cloud Security Alliance [2010] Top Threats to Cloud Computing V1.0 March 2010 y research deliverables CSA will release in 2010.

[8]Glenn A. Bowen [2005] Preparing a Qualitative Research-Based Dissertation: Lessons Learned The Qualitative Report Volume 10 Number 2 June 2005 208-222 http://www.nova.edu/ssss/QR/QR10-2/bowen.pdf

[9]Rolf Johansson [2003] Case Study Methodology - A key note speech at the International Conference.

[10]Sparx Systems [2004] UML TUTORIALS THE USE CASE MODEL copy right reserved © Sparx Systems 2004 published in www.sparxsystems.com.au

[11]Steve Easterbrook, Janice Singer, Margaret-Anne Storey, Daniela Damian [2007] Selecting Empirical Methods for Software Engineering Published for Toronto edu 2007 September.

[12]Ellen Taylor-Powell and Sara Steele [1996] Collecting Evaluation Data Direct Observation published for Program development and evaluation.

[13]CaseMaker [2000] Rapid Application Development @ Copyright 1997-2000 CASEMaker Inc.- E-Book Published in www.casemaker.com

[14]P. Mell and T. Grance, “Draft NIST working definition of cloud computing,” Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009.

[15]M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

[16]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.

[17]Amazon.com, “Amazon s3 availability event: July 20, 2008,” Online at http://status.aws.amazon. com/s3-20080720.html, July 2008.

[18]S. Wilson, “Appengine outage,” Online at http://www.cio-weblog.com/50226711/appengine outage. php, June 2008.

[19]B. Krebs, “Payment Processor Breach May Be Largest Ever,” Online at http://voices.washingtonpost. com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.

[20]G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” Cryptology ePrint Archive, Report 2007/202, 2007, http://eprint. iacr.org/.

[21]M. A. Shah, R. Swaminathan, and M. Baker, “Privacy-preserving audit and extraction of digital contents,” Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.

[22]Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in Proc. of ESORICS’09, Saint Malo, France, Sep. 2009.

[23]Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing,” 2009, http://www.cloudsecurityalliance.org.

[24]H. Shacham and B. Waters, “Compact proofs of retrievability,” in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

[25]Juels and J. Burton S. Kaliski, “Pors: Proofs of retrievability for large files,” in Proc. of CCS’07, Alexandria, VA, October 2007, pp. 584–597.

[26]M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, “Auditing to keep online storage services honest,” in Proc. of HotOS’07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

[27]104th United States Congress, “Health Insurance Portability and Accountability Act of 1996 (HIPPA),” Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996, last access: July 16, 2009.

[28]D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and verifiably encrypted signaturesfrom bilinear maps,” in Proc. of Eurocrypt 2003, volume 2656 of LNCS. Springer-Verlag, 2003, pp. 416–432.