ISSN(Online): 2395-7638

International Journal of Recent Research in Science, Engineering and Technology

Vol. 1, Issue 2, May 2015

Cloud Computing Security Problem in Web - Survey

K.Anbazhagan[1], R. Sugumar[2]

Research Scholar, St. Peter's University , Avadi, Chennai, Tamil Nadu,India[1]

Associate Professor, Department of CSE, Vel Multitech Engineering College, Chennai ,Tamil Nadu,India[2]

ABSTRACT : Cloud Computing is an environment for providing information and resources that are delivered as a service to end-users over the Internet on demand. Thus cloud enables users to access their data from any geographical locations at any time and also has brought benefits in the form of online storage services. Cloud storage service avoids the cost expensive on software, personnel maintenance and provides better performance, less storage cost and scalability. But the maintenance of stored data in a secure manner is not an easy task in cloud environment and especially that stored data may not be completely trustworthy. Cloud delivers services through internet which increases their exposure to storage security vulnerabilities. However security is one of the major drawbacks that preventing several large organizations to enter into cloud computing environment. This work surveyed on several existing cloud storage frameworks, techniques and their advantages, drawbacks and also discusses the challenges that are required to implement secure cloud data storage. This survey results help to identify the future research areas and methods for improving the existing drawbacks.

KEYWORDS: Cloud, Data Dynamics and Third party auditing.

I INTRODUCTION

Cloud Computing is a kind of computing whereby shared resources and IT-related capabilities are provided as a service to outer customers using Internet techniques. Cloud Computing depends on sharing information and computing resources instead of using local servers or personal devices for to manage supplications. Cloud Computing has began to receive mass attract in corporate organizations as it makes the data center be able to work like the Internet to share and access resources in safe and secure manner. To provide data storage service, Cloud Computing utilizes network of enormous amount of servers generally running lower cost customer PC technology with peculiar connections to disperse data processing tasks across end users.

Reason for moving into Cloud is simply because of Cloud allows users to access applications from anywhere at any time through internet. But in past, consumers run their programs and applications from software which downloaded on physical server in their home or building. Cloud provides benefits such as flexibility, disaster recovery, software updates automatically, pay-per-use model and cost reduction. However Cloud also includes major risks such as security, data integrity, network dependency and centralization. When storing customer's data into cloud data storage, security plays a vital role. Sometimes customers store some sensitive information in cloud storage environment. This causes some serious security issues. So providing security to such sensitive information is one of the difficult problems in Cloud computing. In preceding works, several methods are proposed for securely storing data into Cloud. This paper discussed those methodologies and various techniques to effectively store data. Also analysed the advantages, drawbacks of those techniques and provides some directions for future research work.

ISSN(Online): 2395-7638

International Journal of Recent Research in Science, Engineering and Technology

Vol. 1, Issue 2, May 2015

II Storage Techniques in Cloud Computing

2.1 Data Security in Cloud

Providing implicit Storage Security to data in Online is more beneficial in a cloud environment. Presented implicit storage security architecture for storing data where security is disseminated among many entities [1] and also look at some common partitioning methods. So data partitioning scheme is proposed for online data storage that involves the finite field polynomial root. This strategy comprises of two partitioning scheme. Partitioned data are saved on cloud servers that are chosen in a random manner on network and these partitions are regained in order to renovate the master copy of data. Data pieces are accessible to one who has knowledge of passwords and storage locations of partitioned pieces.

2.2 Integrity based Validation

In Cloud Computing, resources and services are distributed across numerous consumers. So there is a chance of various security risks. Therefore authentication of users as well as services is an important requirement for cloud security and trust. When SSL Authentication Protocol (SAP) was employed to cloud, it becomes very complex. As an alternative to SAP, proposed a new authentication protocol based on identity which is based on hierarchical model with corresponding signature and encryption schemes [2]. Signature and encryption schemes are proposed to achieve security in cloud communication. When comparing performance, authentication protocol based on identity is very weightless and more efficient and also weightless protocol for client side.

2.3 Auditing of data in public cloud

Verification of data integrity at unreliable servers is the major concern in cloud storage. Proposed scheme first focused to discover the potential security threats and difficulties of preceding works and build a refined verification scheme Public auditing system with protocol that supports complete dynamic data operations is presented [3]. To accomplish dynamic data support, the existent proofread of PDP or PoR scheme is improved by spoofing the basic Markle Hash Tree (MHT). Proposed system extended in the direction of allowing TPA to perform many auditing jobs by examining the bilinear aggregate signature technique.

2.4 Third Party Auditing (TPA)

Cloud consumers save data in cloud server so that security as well as data storage correctness is primary concern. A novel and homogeneous structure is introduced [4] to provide security to different cloud types. To achieve data storage security, BLS (Boneh–Lynn–Shacham) algorithm is used to signing the data blocks before outsourcing data into cloud. BLS (Boneh–Lynn–Shacham) algorithm is efficient and safer than the former algorithms. Batch auditing is achieved by using bilinear aggregate signature technique simultaneously. Reed-Solomon technique is used for error correction and to ensure data storage correctness. Multiple batch auditing is an important feature of this proposed work. It allows TPA to perform multiple auditing tasks for different users at the same.

2.5 Securing Cloud data

Securely preserving all data in cloud is not an easy job when there is demand in numerous applications for clients in cloud. Data storage in cloud may not be completely trustable because the clients did not have local copy of data stored in cloud. To address these issues, proposed a new protocol system using the data reading protocol algorithm to check the data integrity [5]. Service providers help the clients to check the data security by using the proposed effective automatic data reading algorithm. To recover data in future, also presented a multi server data comparison algorithm with overall data calculation in each update before outsourcing it to server's remote access point.

2.6 Optimal Cloud Storage Systems

ISSN(Online): 2395-7638

International Journal of Recent Research in Science, Engineering and Technology

Vol. 1, Issue 2, May 2015

Cloud data storage which requires no effort is acquiring more popularity for individual, enterprise and institutions data backup and synchronization. A taxonomic approach to attain storage service optimality with resource provider, consumer's lifecycle is presented [9]. Proposed scheme contributes storage system definition, storage optimality, ontology for storage service and controller architecture for storage which is conscious of optimality. When compared with existing work, more general architecture is created that works as a pattern for storage controller. A new prototype NubiSave is also proposed which is available freely and it implements almost all of RAOC concepts.

2.7 Process of access and Store Small Files with Storage

To support internet services extensively, Hadoop distributed file system (HDFS) is acquired. Several reasons are examined for small file trouble of native Hadoop distributed file system: Burden on NameNode of Hadoop distributed file system is enforced by large amount of small files, for data placement correlations are not considered, prefetching mechanism is not also presented. In order to overcome these small size problems, proposed an approach that improves the small files efficiency on Hadoop distributed file system [10]. Hadoop distributed file system is an Internet file system representative, which functioning on clusters. The cut-off point is measured in Hadoop distributed file system's circumstance in an experimental way, which helps to improve I/O performance. From taxonomic way, files are categorized as independent files, structurally and logically-related files. Finally prefetching technique is used to make better access efficiency and considering correlations when files are stored.

2.8 File Security Maintenance

To assure the security of stored data in cloud, presented a system which utilizes distributed scheme [11]. Proposed system consists of a master server and a set of slave servers.There is no direct communication link between clients and slave servers in the proposed model. Master server is responsible to process the client's requests and at slave server chunking operation is carried out to store copies of files in order to provide data backup for file recovery in future. Users can also perform effective and dynamic data operations. Clients file is stored in the form of tokens on main server and files were chunked on slave servers for file recovery. Thus proposed scheme achieved storage correctness insurance and data availability by using Token generation algorithm with homomorphic token and merging algorithm were used.

2.9 File Assured Deletion (FADE) for Secure Storage

Proposed a file assured deletion scheme based on policy to dependably efface files of cancelled file access policies [12]. Working prototype of FADE is implemented at the top of Amazon S3. Performance overhead is also evaluated on Amazon S3.

III CONCLUSION

Cloud Computing is an emerging computing paradigm, allows users to share resources and information from a pool of distributed computing as a service over Internet. Even though Cloud provides benefits to users, security and privacy of stored data in cloud are still major issues in cloud storage. Cloud storage is much more beneficial and advantageous than the earlier traditional storage systems especially in scalability, cost reduction, portability and functionality requirements. This paper presented a survey on secure storage techniques in Cloud Computing. First several storage techniques that provide security to data in cloud have been discussed in detail and also highlighted the necessity for future research on storage methods to provider much better security and accountability. Finally, presented a comparative analysis on storage techniques, that includes the proposed approach, advantages and limitations of those storage techniques.

ISSN(Online): 2395-7638

International Journal of Recent Research in Science, Engineering and Technology

Vol. 1, Issue 2, May 2015

IV REFERENCES

[1] Parakh A, and Kak S (2009). Online data storage using implicit security, Information Sciences, vol 179(19), 3323–3331.
[2] Li H, Dai Y et al. (2009), Identity-Based Authentication for Cloud Computing, M. G. Jaatun, G. Zhao, and C. Rong (Eds.): Cloud Computing, Lecture Notes in Computer Science, vol 5931, 157–166.
[3] Wang Q, Wang C et al. (2011). Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, IEEE Transactions on Parallel and Distributed Systems, vol 22(5), 847–859.
[4] Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400.
[5] Dinesh C (2011). Data Integrity and Dynamic Storage Way in Cloud Computing, Distributed, Parallel, and Cluster Computing.
[6] Kumar S P, Subramanian R (2011). An efficient and secure protocol for ensuring data storage security in Cloud Computing, International Journal of Computer Science Issues, vol 8(6), No 1, 261–274.
[7] Sajithabanu S, Raj E G P (2011). Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(4), 436–440.
[8] Wang C, Wang Q et al. (2012), Toward Secure and Dependable Storage Services in Cloud Computing, IEEE Transactions on Services Computing, vol 5(2), 220–232.
[9] Spillner J, Müller J et al. (2012), Creating optimal cloud storage systems, Future Generation Computer Systems, vol 29(4), 1062–1072.
[10] Kan Yang · Xiaohua Jia" Data storage auditing service in cloud computing:challenges, methods and opportunities", WorldWide Web (2012) 15:409–428 DOI 10.1007/s11280-011-0138-0 Ayad F. Barsoum and M.
[11] Reza Curtmola, Osama Khan, Randal Burns, Giuseppe Ateniese" MR-PDP: Multiple-Replica Provable Data Possession", 1063-6927/08 $25.00 © 2008 IEEE DOI 10.1109/ICDCS.2008.68.
[12] Raghul Mukundan, Sanjay Madria, Mark Linderman" Replicated Data Integrity Verification in Cloud", IEEEcase number 88ABW-2012-6360
[13] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE,Wenjing Lou, Senior Member, IEEE, and Jin Li"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" 1939-1374/12/$31.00 _ 2012 IEEE Published by the IEEE Computer Society).
[14] Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin" Ensuring Distributed Accountability For Data Sharing in the Cloud", 1545-5971/12/$31.00 _ 2012 IEEE Published by the IEEE Computer Society.
[15] Kan Yang, Student Member, IEEE, Xiaohua Jia, Senior Member, IEEE" An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing ",Digital Object Identifier 10.1109/TPDS.2012.278 1045-9219/12/$31.00 © 2012 IEEE