IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 3, Mar 2014, 69-72

IDENTIFICATION OF MISBEHAVING CLOUD SERVER USING TOKEN COMPUTATION

J. KUMARAN[1], ALLAMPATI RAKESH[2] & PAWAR AJIT TANAJI[3]

[1]Assistant Professor, Pondicherry Engineering College, Puducherry, India

[2,3]M.Tech, Department of CSE, Pondicherry Engineering College, Puducherry, India

ABSTRACT

"Cloud computing" became the next generation of IT. The cloud is not simply the latest trendy term for the Internet. Though the Internet is a need for the cloud, the cloud is something more than the Internet. The cloud is where you go to use technology when you need it, for as long as you need it, and not a minute more. You do not install anything on your desktop, and you do not pay for the technology when you are not using it. The cloud can be both software and infrastructure. It can be an application you access through the Web or a server that you provision exactly when you need it. So, lot of people paid their attention towards this new era of IT. Automatically certain security problems will arouse, When the number of users using the cloud. They are either from the server of cloud or any attacker which had an interest to steal the users' data. This paper provides a solution to identify the misbehaving and properly not working server using the token computation. It verifies the cloud server with the data which already distributed into the server data storage. The computed token checks the signature of the data in cloud data storage. Based on the result this scheme gives the authentication for the cloud data storage server weather it was working properly or not.

KEYWORDS: Cloud Storage, Computer Technology, Higher Degree of Structure

INTRODUCTION

Cloud computing is completely real and will affect almost everyone. In this day and age, we have all become stakeholders in the computing movement, and we are all affected when major changes occur. Remember how things changed when the Internet came along? Changes in computer technology seem to move at lightning speeds. It should be no surprise that another evolution is upon us once again, as there have been several since the dawn of the information age.

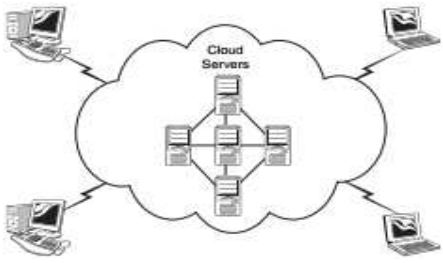

Figure 1: Cloud Computing

Now this paper focuses on why and how these resources should be secured in the Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) environments and offers security "best practices" for service providers and enterprises that are in or are contemplating moving into the cloud computing delivery model. Cloud storage enables you to "throw" data into the cloud and without worrying about how it is stored or backing it up.

When you need it again, you simply reach into the cloud and grab it. You don't know how it is stored, where it is stored, or what has happened to all the pieces of hardware between the time you put it in the cloud and the time you retrieved it. As with the other elements of cloud computing, there are a number of approaches to cloud storage on the market. In general, they involve breaking your data into small chunks and storing that data across multiple servers with fancy checksums so that the data can be retrieved rapidly, no matter what has happened in the meantime to the storage devices that comprise the cloud. Operationally, cloud storage and traditional network storage serve very different purposes. Cloud storage tends to be much slower with a higher degree of structure, which often renders it impractical for runtime storage for an application, regardless of whether that application is running in the cloud or somewhere else. Cloud storage is not, generally speaking, appropriate for the operational needs of transactional cloud-based software. Later, we discuss in more detail the role of cloud storage in transaction application management. For now, think of cloud storage as a tape backup system in which we never have to manage any tapes. In this paper chapter 1 gives the introduction about the cloud computing and the cloud data storage. Chapter 2 gives the survey about the work done by the predecessors. Chapter 3 gives the working methodology of the present scheme and finally Chapter 4 concludes the paper with the inclusion of a future work in it.

RELATED WORK

Ari Juels[2] described a Proofs' of Retrievability (POR) model to ensure the outsourced user data security. This method detects data corruptions of users data and, achieves the guaranty of file retrievabilty. Shacham introduced a new model of POR, which enables unlimited no of queries for public correctness with less overhead. KennadiD[3] proposed a framework for the design of POR. It improves the JK and SW models. All the schemes produce weak security, because they work only for single server. Later, in their subsequent work, Kennadi Brow introduced a HAIL protocol, which extended the POR schemes on multiple servers.

HAIL achieves the integrity and availability of data in cloud. However, this protocol will not address all the data security threats. Ateniese[4] described a Provable Data Possession (PDP) to verify the integrity of outsourced data; it detects the large fraction of file corruption, but no guaranty of file retrivability. In their subsequent work R.D. Pietro proposed a Scalable Data Possession (SDP), this scheme overcomes all problems in the PDP scheme, but this scheme also works only for single server. Later, Curtomola described a Multiple Replica-Provable Data Possession (MR-PDP), which is an extension of PDP to ensure data availability and reliability of outsourced data on multiple servers. Compare to PDP, it requires only single set of tags to challenging servers. In other existing works. Lillibridge [11] proposed a new Internet based backup technique to store client data. It protects data from free riders and disrupter attacks. However, it can't detect data modifications or data changes. Schwarz [5] presents a new model to check the security of data in distributed storage system. It verifies the large amount of data with minimum bandwidth in distributed storage systems. However, in this scheme server can access linear no of file blocks per each challenge.

Filho describes a secured hash function to prevent cheating in a peer-to-peer systems, however it is unusable when data is large. To verify data integrity using RSA-based hash for data possession in peer-to-peer file sharing networks was defined by D. L. G. Filho and P. S. L. M. Barreto in 2006 [12]. However, their scheme requires exponentiation over the entire data file, which is clearly impractical for the server whenever the file is large. Shah [6], proposed a new scheme, which allows Third Party Auditor (TPA) to keep on-line storage honesty with hash values computed by user on encrypted

file. However, this scheme works only for encrypted files. Chen et al. [9] proposed an effective and novel scheme about the third party auditor for cloud data storage. It succeeded in moving the TPA function into the CSP architecture and make it more security.

This construction rapidly reduces the time of response and the usage of data during the communication between the TPA and the CSP. But it needs an integration of TPA into the CSP needs to maintain the separate storage for the TPA and It doesn't provide the Dynamic data operations on the users' data in a secure mode. A new efficient means of polynomial in the size of the input was proposed by M. A. Shah, R. Swaminathan, and M. Baker during the year 2008 in "Privacy Preserving audit and extraction of digital contents"[10]. The main threat from the Third party auditor is that it may kept important information from the auditing process that can compromise the privacy of the user[8]. Anwar hasan[7] proposed scheme that allows the owner to outsourced sensitive data to a CSP, and perform fully block to block dynamic operations on the stored data like block modification operation, insertion operation, deletion operation, and append operation etc.., and it enables mutual trust between the owner and the Cloud Service Provider. But it doesn't discussed about the security of the users data in cloud computing.

DESIGN METHODOLOGY

In this present scheme, first the users' data or files distributed into the cloud data storages in which the user had to check the behaviour of the server. Prepare a token [1] which we can compare it with the signature of the data or file already we have distributed in the cloud servers. The signature of the distributed data in cloud servers will be provided by the cloud data storage servers. This signature is either for the total data/file or for the specified blocks of the data/file. The matching of the signature with the already computed token decides the behaviour of the cloud data storage server.

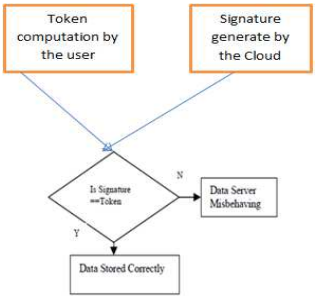

Figure 2: Proposed Scheme Architecture

If the distributed data signature matches with token then the cloud data storage server is working properly, otherwise the server is misbehaving. It means the server is either attacked by the attacker or the third party auditor gleaning the user's data. To identify the localization [1] of the error in server we can check it through the block wise. The recovery of the data is based on the identification of the location of the error point in the data storage cloud server. With this scheme, the identification of the misbehaving server is became so easy. The correctness verification of the cloud server using token computation made differences with the predecessors. This scheme not only verifies the misbehaving serve and also points the location of the error in the data storage. Using this scheme we can retrieve[8] the data easily.

CONCLUSIONS

Cloud computing became the new era of the IT infrastructure. It provides everything as a service. Wherever you are you will get the service from the cloud through internet. Several servers providing storage service to store the users

important data in their cloud. They are all maintaining their separate or third party auditors to keep the users data safely from the attackers or unsecure processing's. Automatically certain security problems will arouse, When the number of users using the cloud. They are either from the server of cloud or any attacker which had an interest to steal the users' data. This paper provided a perfect solution to identify the misbehaving and properly not working server using the token computation. It also locates the error block for retrieving the important user data from the misbehaving server. We have given various possible directions for future research on this cloud computing technology. The most favourable one we believe is a model in which public verifiability is required. Public verifiability, allows Third Party Auditor to audit the cloud data storage without trying to use users' time and outsourced data. We can also allow the dynamic operations in the various blocks of the data in cloud server with the trustful manner.

REFERENCES

1. Cong Wang, Qian Wang, and Kui Ren, and Wenjing Lou, "Ensuring Data storage Security in Cloud Computing". In IWQoS, USA, July 2009.
2. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," *Proc. of CCS '07*, Vol. 53, pp. 584– 597, 2007.
3. K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology e Print Archive, Report 2008/175, 2008.
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," *Proc. Of CCS '07*, Vol. 42, pp. 598–609, 2007.
5. T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," *Proc. of ICDCS '06*, Vol. 26, pp. 12–12, 2006.
6. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," *Proc. 11th USENIX Workshop on Hot Topicsin Operating Systems (HOTOS'07)*, Vol. 13, pp.1–6, 2007.
7. Ayad Barsoum and Anwar Hasan" Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems". IEEE Trans. On parallel and Distributed Systems. Vol. 53, pp, no. 99, 2012.
8. Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance". Proc. of IEEE INFOCOM, 2009.
9. J. Feng, Y. Chen, and D. H. Summerville, "A fair multi-party non-repudiation scheme for storage clouds," in 2011 International Conference on Collaboration Technologies and Systems, Vol. 48, pp. 457– 465, 2011.
10. M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology e Print Archive, Report 2008/186, 2008, http://eprint.iacr.org/.
11. 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), Vol. 34, pp. 29–41, 2003.
12. D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.