International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-3, June 2015
ISSN: 2395-3470
www.ijseas.com

Review of Passive Security Measure on Trusted Cloud Computing

Meenu Bhati[1], Puneet Rani[2]

[1]M.tech,cse,srcem,mdu rohtak,India

[2]M.tech, cse, srcem, A.P, India

ABSTRACT

The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be un-trusted which is under the trusted cloud computing. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, 'inter-clouds" or "clouds-of-clouds" has emerged recently with the trust relationship models ensuring the trusted and trusting resource sharing. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its availability to reduce security risks under the trusted clouds known as reactive security ensuring the data protection to the cloud computing user under the trusted cloud computing.

Keywords-Cloud Computing, Trusted Cloud Computing and Reactive security measures.

INTRODUCTION

In the current era of digital world, various organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. Therefore, storage-as-a-service offered by Trusted Cloud Service Providers emerged as a solution to mitigate the burden of large local data storage and reduce the maintenance cost by means of outsourcing data storage. Since the data owner physically releases sensitive data to a remote Trusted Cloud Service Providers, there are some concerns regarding confidentiality feature can be guarantee by the owner via encrypting the data before outsourcing to remote servers. For verifying data integrity over cloud servers, researchers have proposed provable data possession technique

to validate the intactness of data stored on remote sides. Commonly, traditional access control techniques assume the existence of possession in networked information systems such as those related to critical infrastructures (power facilities, airports, data vaults, defense systems, and so forth) is a matter of crucial importance.[3] Scalable and efficient provable data possession : Storage outsourcing is a rising trend which promotes a number of interesting security issues, many of which have been extensively investigated in the past.[4] Dynamic provable data possession: as storage outsourcing services and resource-sharing networks have become popular, the problem of efficiently proving the integrity of data stored at un-trusted servers has received increased attention. In the provable data possession (PDP) model, the client pre-processes the data and tehn sends it to an un-trusted server of storage, while keeping a small amount of meta-data. The client later ask the server to prove that the stored data has not been tampered with or deleted(without downloading the actual data).[5] Enabling public very fiability and data dynamics for storage security in cloud computing: Cloud Computing has been in visioned as next-generation architecture of IT Enterprise. It moves the application software and data basis to the centralized large data centres, where the management of the data and services may not be fully trustworthy. This works studies the problem of ensuring the integrity of data storage in Cloud Computing.

SYSTEM COMPONENETS AND RELATIONS

The cloud computing storage model considered in this work consist of four main componenets as illustrated in Figure 1: (i) a data owner that can be an organization generating sensitive data to be stored in the cloud and made available for control external use; (ii) a Trusted Cloud Service Providers who manages cloud servers and provides paid storage space on its infrastructure to store the owners files and make them available for authorized users ; (iii) authorized users- a set of owners clients who have the right to access the remote data; and (iv) a trusted third party, an entity who is trusted by all other system componenets and has capabilities to detect /specified dishonest parties.

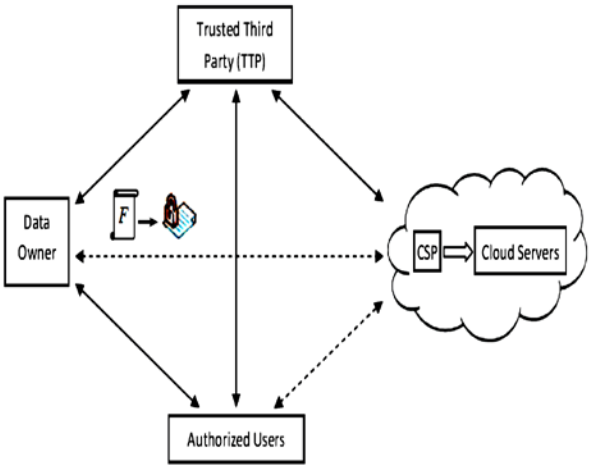

Fig.1: cloud computing data storage system model

In Figure1, the relations between different system componenets are represting by double-sided arrows, where solid and dashed

arrows represent trust and distrust relation, respectively. For example, the data owner , the authorized users, and the Trusted Cloud Service Providers trust the Trusted Third Party. On the other hand, the data owner and authorized users have mutual distrust relations with Trusted Cloud Service Providers. Thus, the Trusted Third Party is used to enable *indirect* mutual trust between these three components. There is a direct trust relation between the data owner and the authorized users Outsourcing, updating and accessing. The data owner has a file F consisting of *m* blocks. For confidentiality, the owner encrypts the data before sending to cloud servers. After data outsourcing, the owner can interact with the Trusted Cloud Service Providers to perform *block-level* operations on the file. In addition, the owner enforces access control by granting or revoking access rights to the outsourced data. To access the data the authorized user send a data-access request to the Trusted Cloud Service Providers, and receive the data file in a encrypted form that can be decrypted using a secret key generated by the authorized user(more detail should be explained later). The Trusted Third Party is an independent entity and thus no incentives to pollute with any party. However, any possible leakage of data towards the Trusted Third Party must be prevented to keep the outsourced data private. The Trusted Third Party and the Trusted Cloud Service Providers are always online, while the owner is *intermittently* online. The authorized users are able to access the data file from the Trusted Cloud Service Providers even when the owner is offline,

Threat model. The Trusted Cloud Service Providers is un-trusted, and thus the confidentiality and integrity of data in the cloud may be at risk. For economic incentives and maintaining a reputation, the Trusted Cloud Service Providers may hide data loss or reclaim storage by discarding data that has not been or is rarely accessed. To save the computational resources, the Trusted Cloud Service Providers may totally ignore the data-update request, or execute just a few of them. Hence, the trusted cloud service providers may return the damaged or stale data for any access request from the authorized users. Furthermore, the Trusted Cloud Providers may not honor the access rights created by owner and permit unauthorized access for misuse of confidential data. On the other hand, a data owner authorized users may collude and falsely accused the Trusted Cloud Service Providers to get a certain amount of reimbursement. They may dishonestly claim that data integrity over cloud server have been violated, or the Trusted Cloud service Providers has returned a stay file that does not match the most recent modification issued by the owner. Security requirements are *Confidentiality:* outsourced data must be protected from the Trusted Third Party, the Trusted Cloud service Providers, and users that are not granted access. *Integrity:* outsourced data is required to remain intact on cloud servers.

The data owner and authorized users must be enable to recognize data corruption over the Trusted Cloud Service Providers side. *Newness:* receiving the most recent version

of the outsourced data file is an imperative requirement of cloud-based storage systems. There must be a detection mechanism if the Trusted Cloud Service Providers ignores any data-update requests issued by the owner. *Access Control:* only authorized users are allowed to access the outsourced data. Revoked users can read unmodified data, however, they must not be able to read updated/new blocks. Trusted Cloud Service Providers *defence:* the Trusted Cloud Service Providers must be safeguarded against false accusations that may be claimed by dishonest owner/users, and such a malicious behavior is required to be revealed.

RELATED WORK

Existing research close to the work can be found in the areas of integrity verification of outsourced data, cryptographic file systems in distributed networks, and access control of outsourced data. Based on proxy re-encryption have introduced a secure distributed storage protocol, in their protocol, a data owner encrypts the blocks with symmetric data keys, which are encrypted using a master public key. The data owner keeps a master private key to decrypt the symmetric data keys. Using the master private key and the authorized user's public key, the owner generate proxy re-encryption keys. A semi-trusted server then uses the proxy re-encryption keys to translate a cipher test into a form that can be decrypted by a specific granted user, and thus enforces access control for the data.

DISCUSSION: Some aspects related to outsourcing data storage are beyond the setting of both provable data possession, e.g., enforcing access control, and ensuring the newness of data delivered to authorized users. Even in the case of dynamic provable data possession, a verifier can validate the correctness of data, but the server is still able to cheat and return stale data to authorized user after the auditing process is done.

EXISTING SYSTEM

Cloud Providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds", "inter-clouds" or "cloud-of-clouds" under Trusted Cloud Service Providers. How we can ensure that the Trusted Cloud Resource Member is not going to harm the another or other resource member's and there respective resources.

PROPOSED SYSTEM

This paper focuses on the issues related to the data security aspect of cloud computing know are reactive security measure. As data and information will be shared with a third party, cloud computing users want to avoid and un-trusted cloud providers. Protecting private and important information, such as credit card details or a patient's medical

records from attackers or malicious insiders is of critical important. In addition, the potential for migration from a single-cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is, we have proposed a cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the Trusted Cloud Service Providers, but also updating and scaling this data on the remote servers. The proposed scheme enables the authorized users to ensures that they are receiving the most recent version of the outsourced data. Moreover, in case of dispute regarding data integrity/newness, a Trusted Third Party is able to determine the dishonest party. The data owner enforces access control for the outsourced data by combining three cryptographic techniques: broadcast encryption, lazy revocation, and key rotation. We have studied the security features of the proposed scheme. We have investigated the overhead added by a scheme when incorporated into a cloud storage model for *static* data with only *confidentiality* requirement. The storage overhead is ~0.4% of the outsourced data size, the communication overhead due to block-level dynamic changes on the data is ~ 1% of block size, and the communication overhead due to retrieving the data is ~0.2% of the outsourced data size. For a large organization with 105 users, performing dynamic operations and enforcing access control add about 63 milliseconds of overhead. Therefore, important features of outsourcing data storage can be supported without excessive overheads in storage, communication, and computation.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS'07,2007, pp. 598-609.

[2] Z. Hao,S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Transactions on Knowledge and data Engineering, vol. 99, no. PrePrints, 2011.

[3] F. Seb'e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J Quisquater," Efficient remote data possession checking in critical information infrastructures," IEEE Trans. On Knowl. And Data Eng, vol. 20, no.8, 2008.

[4] G. Ateniese, R. D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Networks,2008, pp. 1-10.

[5] C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 213–222.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proceedings of the 14th European Conference on Research in Computer Security, 2009, pp. 355–370.

[7] A. F. Barsoum and M. A. Hasan, "Provable possession and replication of data over cloud servers," Centre For Applied Cryptographic Research, Report 2010/32, 2010. uwaterloo.ca/techreports/2010/cacr2010-32.pdf.

[8]Ayad Barsoum, Anwar Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 12, pp. 2375-2385, Dec. 2013.

[9] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: multiple-replica provable data possession," in 28th IEEE ICDCS, 2008, pp. 411–420.

[10] A. F. Barsoum and M. A. Hasan, "On verifying dynamic multiple data copies over cloud servers," Cryptology ePrint Archive, Report 2011/447, 2011, 2011.

[11] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in *CCS '09:* Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 187–198.

[12] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of Retrievability via hardness amplification," in Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography, 2009.

[13] A. Juels and B. S. Kaliski, "PORs: Proofs of Retrievability for large files," in *CCS'07*: Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[14] H. Shacham and B. Waters, "Compact proofs of retrievability," in *ASIACRYPT '08*, 2008, pp. 90–107.

[15] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases. ACM, 2007, pp. 123–134.

[16] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases,"Trans. Storage, vol. 2,no. 2, 2006.

[17] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in NDSS, 2005.