International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 1, Volume 2 (January 2015) www.ijirae.com

Study of Providing Security for Cloud Storage System

Jayshree Shinde*
Information technology & Pune University

Prof-U.R.Godase
Computer Science and Engg & Pune University

Abstract— Cloud computing is a forthcoming revolution in information technology industry because of its performance, accessibility, low cost and many other luxuries. It provides storage for data and faster computing to customers over the internet. That is why companies are reluctant to deploy their business in the cloud even cloud computing offers a wide range of luxuries. Security of data in the cloud is one of the major issues which acts as an obstacle in the implementation of cloud computing. The management of such huge amount of data is quite expensive due to the requirements of high storage capacity and qualified personnel. Storage-as-a-Service offered by cloud service providers is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. A cloud-based storage scheme allows the data owner to benefit from the facilities offered by the cloud service provider and enables indirect mutual trust between them. There are two important features first is, it allows the owner to outsource sensitive data to a cloud service provider, and it ensures that only authorized users receive the outsourced data. Second, it enables indirect mutual trust between the owner and the cloud service provider.

Keywords— Cloud Computing, Data Security, Storage-as-a-Service, Mutual Trust, Access Control.

I. INTRODUCTION

Cloud is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. Cloud computing is regarded as attention that is considerable from both industry and academia due to a number of important advantages namely: flexibility to scale up and down information technology capacity, low management overhead, cost effectiveness immediate access to a wide range of applications, and mobility which includes the customers that can access information at any location wherever they are, rather than having them to work at their workplace. A large pool of distributed shared computing resources that are virtualized constitutes a Cloud computing which includes and is not limited to , Storage, applications, services, processing power, and network bandwidth, , memory .The different types of services that are provided by Cloud Service Providers are Application-as-a-Service, Storage-as-a-Service (SaaS), and Platform-as-a-Service which helps in organizations in concentrating on their core business and leave all their IT operations to experts.

In this era where everything is digitally handled, number of organizations produces a large amount of sensitive data which includes electronic health records, personal information, and also financial data. The management of such a large amount of data locally is problematic, risky and very costly due to the requirement of a qualified personnel and large storage capacity .This is the reason why, Storage-as-a-Service is offered by cloud service providers is now emerged as a solution to lower the load and burden of large local data storage and decrease the cost of maintenance by adopting the means of outsourcing the data storage. By means of outsourcing data the data owners just have to pay the metered fees that are priory decided and are metered in GB/month formats generally. This feasibility helps the data owners to keep the data more on the remote devices than locally. This results in the way that all the authorized users can access the data remotely irrespective of the geographic location that is convenient to them. Since the data owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers. The proposed model provides trusted computing environment by addressing the issues that are more important and are related to outsourcing the data storage which included integrity, confidentiality, mutual trust and access control between the CSP and the data owner. This means that the remotely stored data should be accessed only by legitimate users. The CSP needs to be safeguard from any accusation that is false which may be claimed by a data owner to get illegal compensations.

A. Cloud Computing

The term “cloud” in cloud computing is the communications network or a network combined with computing infrastructure. It is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand .Cloud Computing is a computing platform for sharing resources that include infrastructures, software, applications, and business processes .Cloud Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet.

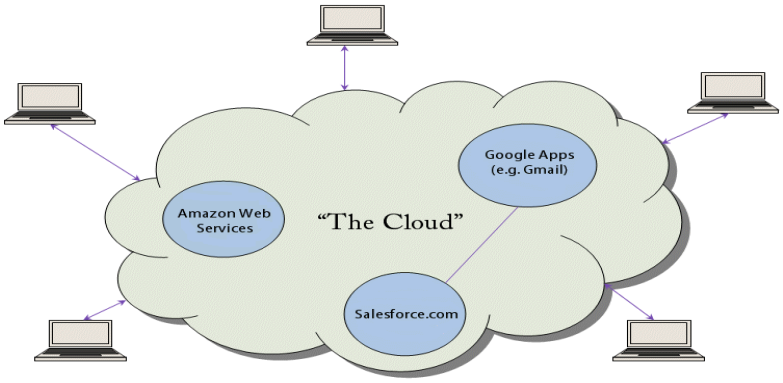

Fig 1: Cloud Computing

II. LITERATURE REVIEW

A. *Introduction*

Existing research can be found in the areas of verification related to storage security on remote servers that are not trusted and access control of outsourced data and integrity of outsourced data. Cloud terminology had already come into existence and in corporate use in 1990s to refer to huge Asynchronous Transfer Mode networks. By 21st century, he term ‘‘cloud computing’’ had appeared, although most of the focus at this time was on Software as a Service. Further in year 1999, sales-force.com was established by Parker Harris, Marc Benioff. They tried with most of the technologies of consumer web sites like Yahoo and Google! to other famous business applications. Not limited to this but also provided the concept’s like “SaaS’’ and ‘‘on demand’’ with their customers. They also interacted the same concept with their business clients. Based as an Infrastructure as a service the Storage as a service (Storing data in cloud) is an one of the important service. The examples that are well known for cloud data storage is Amazon Simple Storage service and Amazon’s Elastic Compute Cloud (EC2). There are also some big challenges that cloud computing faces on the other side and that is important aspect of Quality of Service which includes data storage problem security. The user has no control over data when he puts that into cloud from a local data i.e. unauthorized users could destroy data or modify it and even cloud server collude attacks. Reliability and security are the most factors of which the cloud users are worried about.

B. *Integrity verification*

For verifying data integrity over cloud servers, researchers have proposed provable data possession technique to validate the intactness of data stored on remote sites. A number of PDP protocols have been presented to efficiently validate the integrity of data. Proof of retrievability was introduced as a stronger technique than PDP in the sense that the entire data file can be reconstructed from portions of the data that are reliably stored on the servers. Juels et al. [6] described a formal “proof of retrievability” (POR) model for ensuring the remote data integrity. Their scheme combines spot-checking and error-correcting code to ensure both possession and retrievability of files on archive service systems. Shacham et al. Built on this model and constructed a random linear function based homomorphic authenticator which enables unlimited number of queries and requires less communication overhead.

C. *Data storage security on untrusted remote servers*

The traditional access control techniques used to assume the existence of storage servers and the data owner in the same trust domain. This assumption no longer holds when the data is outsourced to a CSP that is remote and that resides outside the trust domain of the data owner and which takes the full charge of the data management that is outsourced. A feasible solution can be presented to enable the owner to enforce access control of the data stored on a remote untrusted CSP. Through this solution, the data is encrypted under a certain key, which is shared only with the authorized users. The unauthorized users, including the CSP, are unable to access the data since they do not have the decryption key. This general solution has been widely incorporated into existing schemes, which aim at providing data storage security on untrusted remote servers. Kallahalla et al. [8] designed a cryptography-based file system called Plutus for secure sharing of data on untrusted servers. Some authorized users of the data have the privilege to read and write, while others can only read the data. Goh et al. [9] have presented SiRiUS, which is designed to be layered over existing file systems such as NFS (network file system) to provide end-to-end security. To enforce access control in SiRiUS, each data file is attached with a metadata file (md-file) that contains an encrypted key block for each authorized user with some access rights (read or write). More specifically, the md-file represents the d-file’s access control list. The d-file is encrypted using a file encryption key (FEK), and each entry in the ACL contains an encrypted version of the FEK under the public key of one authorized user.

Based on proxy re-encryption, Ateniese et al. 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 generates proxy re-encryption keys. A semi-trusted server then uses the proxy re-encryption keys to translate a cipher text into a form that can be decrypted by a specific granted user, and thus enforces access control of the data. Vimercati et al. [11] have constructed a scheme for securing data on semi-trusted storage servers based on key derivation methods of. In their scheme, a secret key is assigned to each authorized user, and data blocks are grouped based on users that can access these blocks. One key is used to encrypt all blocks in the same group. Moreover, the data owner generates public tokens to be used along with the user's secret key to derive decryption keys of specific blocks. The blocks and the tokens are sent to remote servers, which are not able to drive the decryption key of any block using just the public tokens. The approach in allows the servers to conduct a second level of encryption (over-encryption) to enforce access control of the data. Repeated access grant and revocation may lead to a complicated hierarchy structure for key management.

D. Access control

The concept of over-encryption to enforce access control has also been used by Wang et al. [5] in their scheme; the owner encrypts the data block-by-block, and constructs a binary tree of the block keys. The binary tree enables the owner to reduce the number of keys given to each user, where different keys in the tree can be generated from one common parent node. The remote storage server performs over-encryption to prevent revoked users from getting access to updated data blocks. Another class of solution utilizes attribute-based encryption to achieve fine-grained access control. However these schemes do not implement trust that is mutual between the remote servers and the data owner. Different approaches have been investigated that encourage the owner to outsource the data, and offer some sort of guarantee related to the confidentiality, integrity, and access control of the outsourced data. These approaches can prevent and detect malicious actions from the CSP side. On the other hand, the CSP needs to be safeguarded from a dishonest owner, who attempts to get illegal compensations by falsely claiming data corruption over cloud servers. This concern, if not properly handled, can cause the CSP to go out of business. In this work, a scheme is proposed which will address some major issues related to the storage of data outsourcing which includes access control, confidentiality and integrity. One more imperative issue between the CSP and data owner is the Mutual trust that is addressed in the proposed scheme. A procedural theme is introduced to identify the dishonest party, i.e., any behavior that is irrelevant from any side will be detected and the responsible party will be identified. The proposed cloud-based storage scheme has the following feature first is it allows a data owner to outsource the data to a Cloud Service provider, and it will ensures that only legitimate users receive the data that is outsourced i.e. It will take a guarantee of the access control of the data that is outsourced. Second is it establishes indirect trust that is mutual between the CSP and the data owner since each party resides in a different trust domain.

III PROPOSED IDEA

In cloud storage system, if the CSP receives file from trusted entity other than the owner, the signature verification is not needed since the trusted entity has no incentive for repudiation or collusion. Therefore, delegating small part of owner's work to the TTP reduces both the storage and computation overheads. However the outsourced data must be kept private and any leakage of data toward the TTP must be prevented. A cloud-based storage scheme will allow the owner of the data to benefit from the services offered by the Cloud service provider and enable mutual trust between them. The proposed scheme has two major and highlighted features, first is it allows the owner to outsource data that is sensitive to a Cloud Service Provider, and it also ensures that only users that are authorized receive the data that is outsourced. Further, it enables indirect mutual trust between the Cloud service provider and the data owner.

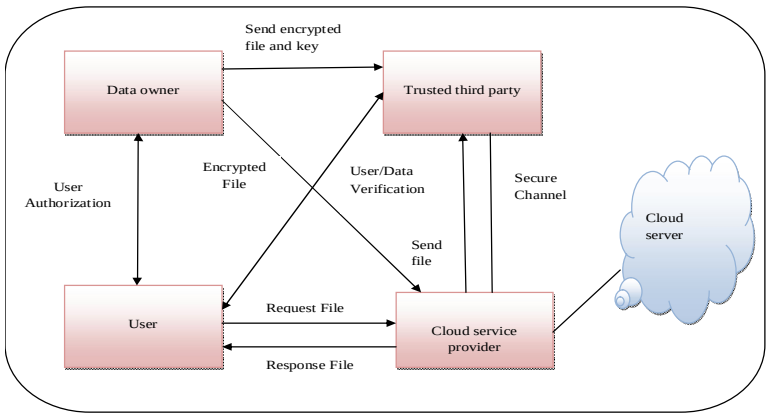

Fig 2: System Architecture

IV CONCLUSION

The proposed scheme is cloud-based storage system which supports outsourcing of data, where the owner is capable of accessing and archiving the data stored by the Cloud Service Provider .It allows owner to benefit from facilities offered by the CSP and enables indirect mutual trust between them. It enables data owners to release their concerns regarding confidentiality, integrity, access control of the outsourced data. To resolve disputes that may occur regarding data integrity, a trusted third party is invoked to determine the dishonest party (owner/users or CSP). The security features of the proposed scheme are studied, and showed that the scheme satisfies the data confidentiality based on the security of underlying encryption algorithm, detection of data integrity violation based on the primate and second-primate resistance properties of the utilized cryptographic hash function, enforcement of access control based on, TTP gives encrypted key to only authorized users and only authorized users can decrypt this key and get the key to read the outsourced data; and detection of dishonest owner/user through a trusted third party.

V FUTURE WORK

The area of cloud computing has attracted many researchers from diverse fields; however, much effort remains to achieve the wide acceptance and usage of cloud computing technology. A number of future research directions stem from our current research. Below, we summarize some problems to address during our future research.

A. User authentication for cloud computing systems

The development of cloud computing encourages the use of resource-constrained devices (PDA/cell phones) on the client side. Thus, rather than local data storage and software installation, users will be authenticate to access data and use applications from the cloud. Such computing model makes software piracy more difficult and enables centralized monitoring. Although cloud computing architecture stimulates mobility of users, it increases the need of secure authentication. Relying on passwords for user authentication is not an efficient approach for sensitive data/applications on the cloud. Passwords is a major point of vulnerability in computer security; they are often easy to guess by automated programs running dictionary attacks, users cannot remember very long passwords, and the common use of meaningful passwords makes them subject to dictionary attacks. Implicit authentication is another interesting area of research to address user authentication problem. One can use learning algorithms to construct a model for the user based on previous behavior patterns, and then compare the recent behavior with the user model to authorize legitimate users. This may require collaboration with researchers from computer science to develop efficient learning algorithms using artificial intelligence, machine learning, and neural networks tools.

B. Outsourcing computation to untrusted cloud servers

Outsourcing computation is a growing desire for resource-constrained clients to benefit from powerful cloud servers. Such clients prefer to outsource computationally-intensive operations (e.g., image processing) to the cloud and yet obtaining a strong assurance that the computations are correctly performed. To save the computational resources, a dishonest CSP may totally ignore the computations, or execute just a portion of them. Sometimes the computations outsourced to the cloud are so critical that it is essential to preclude accidental errors during the processing. The ability to verify computations and validate the returned results is a key requirement of cloud customers. Another imperative point is that the amount of work performed by the clients to verify the outsourced computations must be substantially cheaper than performing the actual computations on the client side. One direction of future research is to investigate the area of verifiable computations and outsourcing computational tasks to untrusted cloud servers. It is also interesting to address mutual trust feature, so a client who receives incorrect results from cloud servers can detect and prove this misbehaviour. Moreover, a dishonest client must not be able to falsely accuse a CSP and claim that the outsourced computations are malformed.

VI REFERANCES

[1] Amazon.com, “Amazon Web Services (AWS),” Online at http://aws.amazon.com, 2008.
[2 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.
[3] 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 Netowrks, 2008, pp. 1–10.
[4] 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.
[5] 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.

[6] 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.
[7] H. Shacham and B. Waters, "Compact proofs of retrievability," Cryptology Print Archive, Report 2008/073, 2008, http://eprint.iacr.org/.
[8] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proceedings of the FAST 03 Conference on File and Storage Technologies. USENIX,2003.
[9] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proceedings of the Network and Distributed System Security Symposium, NDSS. The Internet Society, 2003
[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proceedings of the Network and Distributed System Security Symposium, NDSS. The Internet Society, 2005.
[11] 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.
[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, ser. CCS '06. ACM, 2006, pp. 89–98.
[13] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings of the 29th conference on Information communications, ser. INFOCOM'10. IEEE Press, 2010, pp. 534–542.
[14] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, "Enabling security in cloud storage SLAs with cloud proof," in Proceedings of the 2011 USENIX conference on USENIX annual technical conference, ser. USENIXATC'11. USENIX Association, 2011
[15] M. Blaze, G. Bleumer, and M. Strauss,"Divertible protocols and atomic proxy cryptography," in EUROCRYPT, 1998, pp. 127–144.
[16] M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and efficient key management for access hierarchies," in Proceedings of the 12th ACM Conference on Computer and Communications Security, ser. CCS '05. ACM, 2005, pp. 190–202.
[17] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in Proceedings of the 2009 ACM workshop on Cloud computing security, ser. CCSW '09. ACM, 2009, pp. 55–66.
[18] Rampal Singh, Sawandzzb Kumar, Shani Kumar Agrahari, "Ensuring Data Storage Security in Cloud Computing," International Journal Of Engineering And Computer Science, Volume 2, pp. 825-830, Issue 3March 2013.
[19] Vinaya. V,Sumathi. P, "Implementation of Effective Third Party Auditing for Data Security in Cloud," International Journal of Advanced Research in Computer Science and Software Engineering, Volumes 3, Issue 5, May 2013.
[20] Cong Wang, Qian Wang, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage,"IEEE Transactions on Parallel and Distributed System,Vol 22,N0 5, may 2011.
[21] Roshan R. Kolte, Rahul Deshmukh, Niraj V. Telrandhe, "CPDP Scheme to Provide Data Integrity in Multicloud," International Journal of Computer Applications Volume 83 – No 10, December 2013.

