Privacy Preservation Protocol for Data Storage in Cloud Computing

Meenu Tahilyani[1], Dr. Amit Dutta[2], Dalima Parwani[1]
[1,3]Dept of Computer Science, Sant Hirdaram Girls College, Bhopal (M.P.) India.
[2]Dept of Computer Science & Application, BU, Bhopal Bhopal (M.P.) India.

ABSTRACT
In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. However, this new paradigm of data hosting service also introduces new security challenges. Information owners must trust cloud providers for all of their security. Since various protocols are implemented for the security of these cloud data Storage. But there is a need of privacy preserving protocol that should keep owner's data confidential against the auditor and verify the correctness of data and user. The proposed methodology provides a secure, dynamic auditing and privacy preserving protocol for the secure access of the cloud data storage. This methodology is implemented using the hybrid combination of Access Policy and Elliptic Curve based Encryption.

Keyword - Cloud Computing, Cloud Storage, Privacy PreservationProtocol

I INTRODUCTION

Cloud computing presents a new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing dynamically scalable and often virtualized resources as a service over the Internet. Clouds can be explained as pools of virtualized resources that can be easily used and accessed. For optimum resource utilization the resources in cloud can be reconfigured dynamically.Cloud computing basically contains virtualization, on-demand deployment, Internet delivery of services, open source software etc. [1].A technique Cloud Information Accountability (CIA) framework is based on the notion of information accountability. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information accountability focuses on keeping the data usage transparent and traceable [2].

Cloud Computing provides efficient computing by centralizing storage, memory, processing and bandwidth promising lower costs, rapid scaling, easier maintenance, service availability. The main focus needs upon the data security and privacy. Services provided by cloud computing are [3].

(a) Services to large number of distinct end users in opposition to bulk data processing or workflow management for a single user.
(b) Using the data model which consists of sharable units in which all data objects has access control lists (ACLs) with one or more users.
(c) Developers are capable of running applications on a separate computing platform with physical infrastructure, job scheduling, user authentication, base software environment etc. and do not need to implement platform by themselves.

Cloud Computing is based on architecture which is responsible for providing various services and can be categorized into:

(a) Infrastructure as a Service (IaaS) is foundation of cloud services providing clients to access server hardware, use storage services, bandwidth usage & information and other computing resources.
(b) Platform as a Service (PaaS) is builds upon IaaS. It provides clients to access basic operating software. It gives optional services for developing and uses the software applications that are database access and payment service. These services are then not needed to be purchased and the computing infrastructure does not need to be managed.

Software as a Service (SaaS) is builds upon IaaS and PaaS providing clients to access the software applications [4].

II THEORETICAL BACKGROUNDNCLOUD STORAGE

It is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running.

There are three main cloud storage models:

(a) Public cloud storage services, such as Amazon's Simple Storage Service (S3), provide a multi-tenant storage environment that's most suitable for unstructured data.

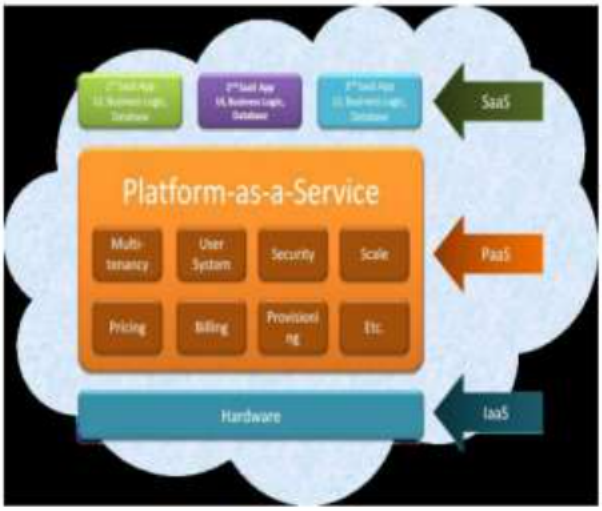

Fig 1. Cloud Computing Services

(b) Private cloud storage services provide a dedicated environment protected behind an organization's firewall. Private clouds are appropriate for users who need customization and more control over their data.
(c) Hybrid cloud storage is a combination of the other two models that includes at least one private cloud and one public cloud infrastructure. An organization might, for example, store actively used and structured data in a private cloud and unstructured and archival data in a public cloud.

An enterprise-level cloud storage system should be scalable to suit current needs, accessible from anywhere and application-agnostic.

III RESEARCH CHALLENGES ON CLOUD STORAGE

In Cloud Computing, data owners may share their outsourced data with a large number of users, who might want to only retrieve certain specific data files they are interested in during a given session. One of the most popular ways to do so is through keyword-based search. Such keyword search technique allows users to selectively retrieve files of interest and has been widely applied in plaintext search scenarios. Unfortunately, data encryption, which restricts user's ability to perform keyword search and further demands the protection of keyword privacy, makes the traditional plaintext search methods fail for encrypted cloud data. Although traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords without first decrypting it, these techniques support only conventional Boolean keyword search, without capturing any relevance of the files in the search result. Ranked search improves system usability by normal matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), as directly outsourcing relevance scores will drips a lot of sensitive information against the keyword privacy.

IV PRIVACY-PRESERVING PROTOCOL

Privacy preservation enables various users to securely transmit their data over cloud network into data storage centers. The main issue that takes place in privacy-preserving is the data privacy. This is because: 1) for public data, the auditor may obtain the data information by recovering the data blocks from the data proof. 2) For encrypted data, the auditor may obtain content keys somehow through any special channels and could be able to decrypt the data. To solve the data privacy problem, our method is to generate an encrypted proof with the challenge stamp by using the bilinearity property of the bilinear pairing, such that the auditor cannot decrypt it, but the auditor can verify the correctness of the proof without decrypting it [5].

V LITERATURE SURVEY

Madhan Kumar Srinivasan [6] analyzed the current security challenges in cloud computing environment based on state-of-the-art cloud computing security taxonomies under technological and process-related aspects.Qian Wang[9]studied the problem of ensuring the integrity of data storage in Cloud Computing. In particular, they consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block medications, insertion and deletion, is also a significany step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public variability or dynamic data operations, this paper achieves both. They first identified the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for seamless integration of these two salient features in our protocol design. In particular, to achieve efficient data dynamics, they improve the Proof of irretrievability model [10] by manipulating the classic Markel Hash Tree (MHT) construction for block tag authentication. Extensive security and performance analysis show that the proposed scheme is highly efficient and provably secure.

Ramgovind S[11] provides an overall security perspective of Cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of Cloud computing. Gartner's list on cloud security issues, as well as the findings from the International Data Corporation enterprise panel survey based on cloud threats, will be discussed in this paper.Q. Wang[12] adopted the block less approach, and authenticate the block tags instead of original data blocks in the verification process. To achieve efficient data dynamics a new and efficient technique is implemented.Srinivas D[13] proposed a new technique in which the burden of cloud user from the tedious and possibly pricey auditing task, but also alleviates the users' terror of their outsourced data security.ZhuYan[14] suggested efficient provable data possession for hybrid clouds. They focused on the construction of PDP scheme for hybrid clouds, supporting privacy protection and dynamic scalability. In 2009 Qian Wang et al [15] introduced a new scheme which gives remote data integrity and verifiability means dynamic data operations. The method initially identifies the troubles and potential security problems of direct extensions with fully dynamic data updates. Seny Kamara and Kristin Lauter [16] considered the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. They survey the benefits such architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage. V.Sathiya Suntharam[17] proposed a method to build a trusted computing environment for Cloud Computing system by providing platform in to Cloud Computing system. In this method some important security services including authentication, encryption and decryption and compression are provided in Cloud Computing system. The need for this software can be categorized in two categories: Encryption and Decryption, Compression. JinWookByun[18]propose an efficient conjunctive keyword search scheme over encrypted data in aspects of communication and storage costs. Concretely, they reduce the storage cost of a user and the communication cost between a user and a data supplier to the constant amounts.

VI CONCLUSION

In the Existing systems, the notion of public audit ability has been proposed in the context of ensuring remotely stored data integrity under different system and security models. Public audit ability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data. However, most of these schemes do not consider the privacy protection of users' data against external auditors. Indeed, they may potentially reveal user's data to auditors. This severe drawback greatly affects the security of these protocols in cloud computing. From the perspective of protecting data privacy, the users, who own the data and rely on TPA just for the storage security of their data, do not want this auditing process introducing new vulnerabilities of unauthorized information leakage toward their data security.

The main objectives of our work are as follows:

(a) To provide privacy-preservation in cloud data storage.

(b) To provides security from various attacks.

(c) To provides less computational cost and time for data storage.

(d) To implement an efficient framework for cloud data storage.

REFERENCES

[1] Pankaj Arora, RubalChaudhary Wadhawani and Er. Satinder Pal Ahuja "Cloud Computing Security Issues in Infrastructure as a Service", International Journal of Advanced Research in Computer Science and Software Engineering, 2012.

[2] Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin "Ensuring Distributed Accountability for Data Sharing in the Cloud", IEEE Transactions on Dependable And Secure Computing, 2012

[3] Dawn Song, Elaine Shi, Ian Fischer and Umesh Shankar "Cloud Data Protection for the Masses", IEEE 2012

[4] Kim-Kwang Raymond Choo "Cloudcomputing: Challenges and future directions", 2010.

[5] Kan Yang," An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEETransactions on Parallel and Distributed Systems, VOL. 24, NO. 9, 2013.

[6] Madhan Kumar Srinivasan,KSaurkesi,Paul Rodrigues,Sai Manoj M,Revathy P." A classification of security challenges in the present cloud computing environment"ICACCI '12, August 2012.

[7] Pengfei Sun, QingniShen,Ying Chen ,ZhonghaiWu,Cong Zhang, Load Balancing based on Multilateral Security in Cloud,CCS, October 17–21, 2011.

[8] LBVM: Load balancing of virtual machine, http://lbvm.sourceforge.net.

[9] Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou. Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing.

[10] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of ASI-ACRYPT'08, pp. 90–107, Springer-Verlag, 2008.

[11] Ramgovind S, Eloff MM, Smith E, The Management of Security in Cloud Computing,IEEE, 2010.

[12] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[13] Srinivas, D. "Privacy-Preserving Public Auditing In Cloud Storage Security" International Journal of computer science and Information Technologies, ISSN: 0975-9646, vol. 2, no. 6, pp. 2691-2693, 2011.

[14] Zhu, Yan, Huaixi Wang, Zexing Hu, Gail-JoonAhn, Hongxin Hu, and Stephen S. Yau, "Efficient provable data possession for hybrid clouds." In Proceedings of the 17th ACM conference on Computer and communications security, pp. 756-758. ACM, 2010.

[15] Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing" Proceedings of the 14th European conference on Research in computer security(ESORICS'09), pp. 355-370, 2009.

[16] Armbrust, Michael, Armando Fox, Rean Seny Kamara and Kristin Lauter, " Cryptographic Cloud Storage", FC 2010 Workshops, LNCS 6054, pp. 136–149, IFCA/Springer-Verlag Berlin Heidelberg 2010

[17] V.SathiyaSuntharam, DR.K.Venkateswara Reddy, N .Puspalatha, "Data Storage Security in Cloud Computing and Verification of Metadata by Encryption", International Journal of Computer Science and Electronics Engineering, December 2012

[18] JinWook Byun, Dong Hoon Lee, and Jongin Lim, "Efficient Conjunctive Keyword Search on Encrypted Data Storage System", EuroPKI 2006, LNCS 4043, pp. 184–196, Springer-Verlag Berlin Heidelberg 2006