SURVEY ON DISTRIBUTED, CONCURRENT AND INDEPENDENT ACCESS TO ENCRYPTED CLOUD IAAS

Afia Abdul Rahman[1] , Liji Samuel[2]
Computer Science and Engineering
Sree Buddha College Of Engineering For Women
Elavumthitta, Pathanamthitta India
afiabtechit@gmail.com

Abstract— Critical data storage at cloud should come with the guarantee of security and also the data must be available at rest, in motion, and in use. Different alternatives are available for storage services, while data confidentiality solutions for the cloud IaaS are still immature. In this architecture, integration of Cloud Infrastructure as-a-Service with data confidentiality is presented. This supports geographically distributed clients to connect directly to an encrypted cloud IaaS. The proposed system eliminates intermediate proxies and so it is possible to limit the availability and scalability properties that are intrinsic in cloud-based solutions.

***Index Terms*— Encryption, Cloud IaaS**

I. Introduction

While considering a cloud context, where critical information is placed in infrastructures of untrusted third parties or cloud service providers, data confidentiality must be ensured and must be taken with great importance. This needs clear data management techniques in which original plain data must be accessible only by trusted parties that do not include cloud providers, intermediaries and internet. Also, in any untrusted context, data must be encrypted. For this purposes, different levels of complexity are to be implemented depending on the type of cloud service. There are several solutions ensuring confidentiality for the storage as a service paradigm. And in some cases, most of encryption schemes protect data confidentiality, but it sometimes limit the functionality of the storage system as a few operations are supported over encrypted data. Inorder to construct a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority.

II. LITERATURE SURVEY

Luca Ferretti, Michele and Mirco proposed a system which is applicable in cloud databases. This was a novel architecture which integrates cloud database services with confidentiality of data and also it is possibile to execute concurrent operations on encrypted data. This supports geographically distributed clients to connect directly to an encrypted cloud database and to execute concurrent and independent operations including those modifying the database structure[1].When considering the cost of data management in such databases, it is a serious issue for normal clients who focus on economical data storage with data security. Direct data retrieval in a distributed computing system include a system for backing up files in a distributed computing system, such as a distributed file system. Here a backup request is initiated with a backup client program to backup a requested file. It is determined that whether the requested file is maintained in a shared name space. The backup client program and a backup server program are capable of accessing files maintained in the shared name space and the file server maintains the files in the shared name space.

Deyan Chen and Hong Zhao proposed a system well-known that cloud computing has many potential advantages and many enterprise applications[2]. Also data are migrating to public or hybrid cloud. The market size the cloud computing shared is still far behind the one expected. From the consumer's perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. This provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. It also discusses some current solutions and describes future research work about data security and privacy protection issues in cloud.

Hsiao-Ying and Tzeng proposed a cloud storage system which consists of a collection of storage servers and it provides long-term storage services over internet . Data storage in a third party's cloud system causes serious concern over data confidentiality. Most of encryption schemes protect data confidentiality, but it sometimes limit the functionality of the storage system as a few operations are supported over encrypted data[3]. Inorder to construct a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. So they proposed a threshold proxy re encryption scheme and integrated it with a decentralized erasure code such that a secure distributed storage system is formulated. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back. The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. This method fully integrates encrypting, encoding, and forwarding.

Guojun Wang, Qin Liu and Jie Wu proposed that cloud computing is an emerging computing paradigm that enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. Especially for small and medium-sized enterprises with limited budgets, can achieve cost savings and productivity enhancements by using cloud-based services to manage projects and also make collaborations[4]. But, allowing cloud service providers (CSPs), which are not in the same trusted domains as enterprise users, to take care of confidential data, may raise potential security and privacy issues. For keeping the sensitive user data confidential against untrusted CSPs, a natural way is to apply cryptographic approaches, by disclosing decryption keys only to authorized users. However, when enterprise users outsource confidential data for sharing on cloud servers, the adopted encryption system should not only support fine-grained access control, but also provide high performance, full delegation, and scalability, so as to best serve the needs of accessing data anytime and anywhere, delegating within enterprises, and achieving a dynamic set of users.

Armbrust, Armando and Griffith published this article with a goal to reduce that confusion by clarifying terms, providing simple figures to quantify comparisons between of cloud and conventional computing, and identifying the top technical and non-technical obstacles and opportunities of cloud computing. According to them, cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services[5]. The services themselves have long been referred to as Software as a Service (SaaS). Some vendors use terms such as IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) to describe their products.

Gansen, Rong, Jin Li and Feng proposed cloud computing has been acknowledged as one of the prevaling models for providing IT capacities. The off-premises computing paradigm that comes in connection with cloud computing has incurred great concerns on the security of data, especially in the integrity and confidentiality of data, as cloud service providers may have complete control on the computing infrastructure that underpins the services[6]. This makes it difficult to share data via cloud providers where data should be confidential to the providers and only authorized users should be allowed to access the data. This paper aims to construct a system for trusted data sharing through untrusted cloud providers, to address the above mentioned issue. The constructed system can imperatively impose the access control policies of data owners, preventing the cloud storage providers from unauthorized access and making illegal authorization to access the data.

Many organizations outsource data storage to the cloud such that a member (owner) of an organization can easily share data with other members (users). Because of security concerns in the cloud, both owners and users are suggested to verify the integrity of cloud data with Provable Data Possession (PDP) before further utilization on data. Some methods either unnecessarily reveal the identity of a data owner to the untrusted cloud or any public verifiers, or introduce significant overheads on verification metadata to preserve anonymity[7]. Boyang, Chow, Ming Li and Hui Li proposed a simple and efficient publicly verifiable approach to ensure cloud data integrity without sacrificing the anonymity of data owners nor requiring significant verification metadata. They introduced a security-mediator (SEM), which is able to generate verification metadata (i.e., signatures) on outsourced data for data owners. This approach decouples the anonymity protection mechanism from the PDP. Thus, an organization can employ its own anonymous authentication mechanism, and the cloud is oblivious to that since it only deals with typical PDP-metadata.

Yang Tang, Lee, Lui and Perlman proposed a system to achieve security goals which is known as FADE that is built upon a set of cryptographic key operations that are self-maintained by a quorum of key managers that are independent of third-party clouds. FADE acts as an overlay system that works seamlessly atop today’s cloud storage services[8]. They implemented a proof-of-concept prototype of FADE atop Amazon S3, one of today’s cloud storage services and conducted extensive empirical studies and demonstrated that FADE provides security protection for outsourced data while introducing only minimal performance and monetary cost overhead. Also providing insights of how to incorporate value-added security features into today’s cloud storage services.

The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. Shucheng, CongWang, Ren and Lou proposed a system that addresses the challenging open issues such as data security and access control on one hand and defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents[9]. This is achieved by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. This scheme also has salient properties of user access privilege confidentiality and user secret key accountability.

References

[1] Luca Ferretti, Michele Colajanni and Mirco Marchetti, Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases, IEEE Transactions On Parallel and Distributed Systems, Vol. 25, No. 2, February 2014

[2] Deyan Chen and Hong Zhao, Data Security and Privacy Protection Issues in Cloud Computing, in ICCSSE International Conference, Vol. 1, March 2012

[3] Hsiao-Ying Lin and Tzeng, A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding , IEEE Transactions On Parallel and Distributed Systems, Vol.23, No. 6, June 2012

[4] Guojun Wang, Qin Liu and Jie Wu , Hierarchical Attribute-Based Encryption for
Fine-Grained Access Control in Cloud Storage Services, ACM 978-1-4503-0244, October 2010

[5] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee and David Patterson, A View of Cloud Computing, ACM, Vol. 53 No. 4, Pages 50-58, 2010

[6] Gansen Zhao, Chunming Rong, Jin Li and Feng Zhang, Trusted Data Sharing over Untrusted Cloud Storage Providers, CloudCom, IEEE Second International Conference, December 2010

[7] Boyang Wang, Chow, Ming Li and Hui Li, Storing Shared Data on the Cloud via Security-Mediator, IEEE 33rd International Conference on Distributed Computing Systems, Pages 124-133, 2013

[8] Yang Tang, Lee, Lui and Perlman, Secure Overlay Cloud Storage with Access Control and Assured Deletion, IEEE Transactions On Dependable and Secure Computing, Vol.9, No. 6, November 2012

[9] Shucheng Yu, Cong Wang, Kui Renand Wenjing Lou, Achieving Secure, Scalable and Fine-grained Data Access Control in Cloud Computing, INFOCOM, IEEE Proceedings, March 2010