Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 60 (2013) 16438-16441

ISSN: 2229-712X

Secure storage of data in cloud

Sai Krishna Manohar

Department of Information Technology, Tirumala Engineering College, Narasaraopet, India.

ARTICLE INFO

Article history:

Received: 3 April 2013;

Received in revised form:

24 June 2013;

Accepted: 13 July 2013;

Keywords

Security,
Data Encryption,
Compression,
Data Decryption,
Authentication,
Decompression,
Collaboration,
Architecture.

ABSTRACT

Cloud computing provides the way to share distributed resource and services that belong to different organizations. Since cloud computing share distributed resources via network in the open environment thus it makes security problems. All types of users who require the secure transmission or storage of data in any kind of media or network. Since, the data transmissions on the internet or over any networks are vulnerable to the hackers attack. I'm in great need of encrypting the data. I propose a method to build a trusted computing environment for cloud computing system. In this method some important security service including authentication, encryption, decryption and compression are provided in the cloud computing system. Need of this software is divided in to three modules: Encryption, Decryption, and Compression.

Introduction

Cloud computing is a great term for anything that involves delivery hosted services over the internet. These services are broadly divided into three categories: infrastructure-as-a-service (IAAS), platform-as-a-service (PAAS), and software-as-a-service (SAAS). A cloud service has three distinct characteristics that differentiate it from traditional hosting. The advantage of cloud is cost savings. The prime disadvantage is security. Cloud Computing is used by many software industries nowadays. Since the security is not provided in cloud, many companies adopt their unique security structure. For example IBM is having its own security structure. Introducing a new and uniform security structure for all types of cloud is the problem I'm going to tackle in this paper. Since the data placed in the cloud is accessible to everyone, security is not guaranteed. I propose a mentioned to build a trusted computing environment for cloud computing system by providing secure cross platform into cloud computing system. In this method some important security services including authentication, encryption, decryption and compression are provided in cloud computing system.

Characteristics

Cloud computing is cost-effective. Here, cost is greatly reduced as initial expense and recurring expenses are much lower than traditional computing. Maintenance cost is reduced as a third party maintains everything from running the cloud to storing the data. Cloud is characterized by features such as platform, location and device independency, which makes it easily adoptable for all sizes of business. In cloud computing security is tremendously improved because of a superior technology security system, which is now easily available and affordable. Another most important characteristic in cloud computing is Scalability, which is achieved through server virtualization. There are some characteristics that are as follows:

1. On-demand Self service

A consumer can unilaterally provision computing capabilities, such as server time and network storage. On-demand self-service allows users to obtain, configure and deploy cloud services themselves using cloud service catalogues, without requiring the assistance of IT.

2. Broad Network Access

Capabilities are available over the network and accessed through standard mechanisms that provide use by heterogeneous thick client platforms.

3. Resource Pooling

The providers computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand..

4. Selection of provider

A good service provider is key to good service. So, it is imperative to select the right service provider. As cloud computing has taken hold, there are four major benefits. Those are anywhere/anytime access, Collaboration among users, Storage as a universal service, Cost benefits.

Critique Appraise:

1. Enabling Public Audit and Data Dynamics for Storage Security in cloud computing

The third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to access the cloud server service security on behave of the user upon request. Users also dynamically interact with the cloud server to access and update their stored data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while existence of a semi-trusted cloud server as done. Most of the time it behaves like properly and doesn't deviate from the prescribed protocol execution. However during providing the cloud data storage

Tele:
E-mail addresses: saikrishnamanohar@gmail.com

based services, for their own benefits the cloud server based services, for their own benefits the cloud server might neglected to keep or deliberately delete rarely accessed data files which belongs to hide the data corruptions caused by server hacks or failure to maintain repudiation. I assume that the TPA, who is the business of audit, is reliable and independent, and thus has no incentive to collude with either the cloud server during the audit process.

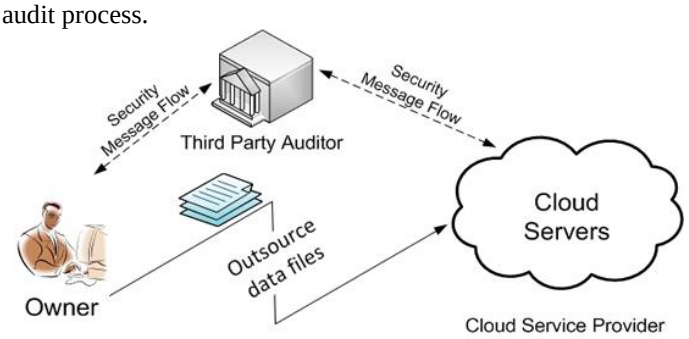

Fig. 1: Architecture of cloud Data Storage

The cloud computing is a model of computing and it is distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers and clients.

2. Achieving Secure, Scalable data access in cloud computing

The proposed scheme enables the data owner to delegate tasks of data files that re-encryption and user secret key update to cloud servers. Without disclosing data contents. I achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. The proposed scheme also has salient features of user access privilege confidentially and user secret properties of user access privilege confidentially and user secret key accountability and achieves fine scalability and data confidentially for data access control in cloud computing. By reviewing the peer analysis my proposal scheme is highly efficient and provably secures under existing security models.

A. Advantages

- Low initial capital investment.
- Shorter start-up time for new services.
- Lower maintenance.
- Lower operation costs.
- Easier disaster recovery.

In order to achieve secure, scalable data in cloud, the author utilize to combine following three advanced cryptographic techniques:

- Key Policy Attribute-based encryption (KP-ABE).
- Proxy re-encryption.
- Lazy re-encryption.

B. Description of three encryptions

(i) Key policy Attribute-Based Encryption (KP-ABE)

KP-ABE is public key encryption cryptography primitive for one-to –many communications. In KP-ABE, data are associate with attributes for each of which a public key component is defined. User secret key is able to decrypt a cipher text if and only if the data attributes satisfy his access structure. A KP-ABE scheme is composed of four algorithms which can be defined as follows:

Setup Attributes

- Encryption
- Secret key generation
- Decryption

(ii) Proxy Re-encryption Policy (PRE)

Proxy Re-encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under person-A public key into another cipher text can be opened by person-B private key without seeing the plaintext [2].

(iii) Lazy Re-encryption

This technique is allows to cloud servers to aggregate computation tasks of multiple operations. The operations such as,

- Update secret keys.
- Update user attributes.

C. Audit secure cloud data storage services publicly

The publicly auditable cloud data storage is able to help this nascent cloud economy become fully established. With public audit, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed. Such an auditing service not only helps save data owners' computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud [3].

D. Online Data Storage with accurate Security

The partitions are stored on randomly chosen servers on the network and they need to be retrieved to recreate the original data. Data reconstruction requires access to each server, login password and the knowledge of the servers on which the partitions are stored. This scheme may also be used for data security in sensor networks and internet voting protocols.

The authors have described an implicit security architecture suited for the application of online storage. In this scheme data is partitioned in such a way that each partition is implicitly secure and does not need to be encrypted. These partitions are stored on different servers on the network which are known only to the user. Reconstruction of the data requires access to each server and the knowledge as to which servers the data partitions are stored. Several variations of this scheme are described, which include the implicit storage of encryption keys rather than the data, and where a subset of the partitions may be brought together to recreate the data.

E. Identity –based authentication for computing in cloud

An identity-based encryption (IBE) and decryption and identity-based signature (IBS) schemes for IBHM CC. Based on the former IBE and IBS schemes, an identity based authentication for cloud computing (IBACC) is proposed. The author presented an identity based authentication for cloud computing, based on the identity-based hierarchical model for cloud computing (IBHMCC) and corresponding encryption and signature schemes. The authors proposed Identity-based Authentication Protocol. Identity-based Authentication Protocol contains sequence of steps. In step (1), the client C sends the server S a Client Hello message. The message contains a fresh random number C n, session identifier ID and C specification. In step (2), the server S responds with a Server Hello message which contains a new fresh random number S n, the session identifier ID and the cipher specification S specification the cipher text is transmitted to C as Server Key Exchange message. Then S generates a signature Sig S as the Identity Verify message to forward to C. Finally, The Server Hello Done message means the step (2) is over. In step (3), C firstly verifies the signature S Sig S with the help of S ID Being certificate-free, the authentication protocol aligned well with demands of cloud computing. Performance analysis indicated that the

authentication protocol is more efficient and lightweight than SAP, especially the more lightweight user side.

F. Security Framework of Cloud Data Storage Based on Multi Agent System Architecture

The authors propose Multi-Agent System (MAS) techniques that can be beneficial in cloud computing platform to facilitate security of cloud data storage (CDS) among it [11]. M.A.S architecture offered eleven security attributes generated from four main security policies of correctness, integrity, confidentially and availability of users' data in the cloud.

G. Privacy-Preserving Public Auditing for Secure Cloud Storage

A Public Auditing Scheme Consists of four algorithms (Key Gen, Sig Gen, Gen Proof, Verify Proof)

(i). KeyGen

Key generation algorithm that is run by the user to setup the scheme

(ii)**. SigGen**

It is used by the user to generate verification metadata, which may consist of MAC, signatures or other information used for auditing.

(iii)**. GenProof**

Run by the cloud server to generate a proof of data storage correctness.

(iv)**. Verify Proof**

Run by the TPA to audit the proof from the cloud server. The author uses homomorphic authenticator technique for aggregate the data..Also uses a random mask technique achieved by a Pseudo Random Function (PRF)

Existing System

To introduce an effective third party auditor (TPA) for privacy and security, the following fundamental requirements have to be met: TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user. The third party auditing process should bring in no new vulnerabilities towards user data privacy. They utilized and uniquely combined the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. This scheme is the first to support scalable and efficient public auditing in the Cloud Computing. In particular, this scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA. The security and performance is justified through concrete experiments and comparisons with the state-of-art. In cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed or even hiding data loss incidents so as to maintain a reputation. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture. Another problem is that data stored in the cloud does not remain static [9].

Proposed System

The Proposed Network consists of three backup sites for recovery after disaster. The backup sites are located at remote location from the main server. If any one of the paths fails it uses alternate path working. The encrypted file will be creating during back up sites and data's are compressed. The data will be decrypted during recovery operation. I proposed a cross platform integration model by using a secure communication via Internet and the utilization of a key for security.

A. Data Backup Operation

Client sends the data to the server which is known as Main Server. At the same time data is also back up to Multi Servers. In this method for data backup it involve with three Multi Server such as (SA 1(Server, Application), SA 2, SA 3, etc…).

B. Operation

Multi-server sends the key ID to our mail id.

C**. Data Encryption and Compression**

The data is to be encrypted and compressed in multi-server. In encryption and compression the data that has to stored in a cloud cannot be stored in a text format due to security reasons so it must be transformed into an encrypted format. The data also has to be compressed for secure transmission. This method deals with the compression and encrypts the data before it is taken as back up in multi server. To encrypt the data's SHA Hash Algorithm is used for compression GZIP algorithm is used and for symmetric splitting of files SFSPL algorithm is implemented.

D. Authentication

Suppose the data is deleted in the client system. Then we authenticate the data through following procedures: Find the key in our email id. Give the file name and date in login form.

E. Data Decryption and Decompression

This method deals with the decompression and decrypting the data after it is taken as back up in multi server. It is automatically created by the server and it is send as email to the user. The data which taken as backup is stored in unrecognizable format, which cannot be open by any user. It can be readable only when it decrypt and decompress the data. If we give the key and data in the next login form, we will get the recovery of specified file.

Fig.2: Data Backup

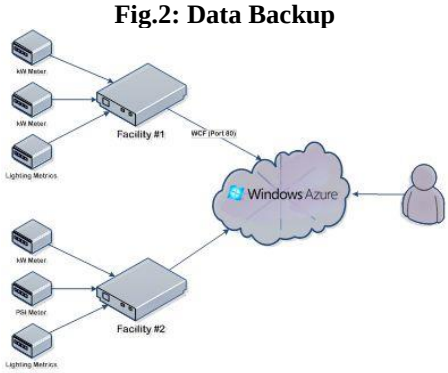

Fig.3: Data Recovery

Conclusion

Authentication is necessary in Cloud Computing. After referred the papers I propose a new idea means Secure Cross Platform Communication in a cloud. Two major obstacles to this

process of data sharing are providing a common storage space and secure access to the shared data. Cloud Databases are an emerging type of non relational databases which do not follow relational algebra and are generally key-value oriented systems which are used for storing internet scale data and provide easy programmatic access. The main goal is to securely store and manage data that is not controlled by the owner of the data. The data are stored in cloud environment Cloud security here is solved by providing an credential for data in the cloud. This credential can be used to retrieve data from the cloud in a secure manner.

References

[1] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li , "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[2] Shucheng Yu., Cong Wang†, Kui Ren†, Wenjing Lou., "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE Communications Society for publication in the IEEE INFOCOM 2010.

[3] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, 2010.

[4]Eoin Gleeson, "Computing industry set for a shocking change," Apr 2009, Money Week, from http://www.moneyweek.com/investment-advice/ computing-industryset- For-a-shocking-change-43226.aspx

[5] http://en.wikipedia.org/wiki/Cloud_storage

[6] Eucalyptus systems, http://eucalyptus.cs.ucsb.edu!.

[7] Enomalism elastic http://www.enomaly.com. Computing infrastructure, http://www.springerlink.com

[8] Sales force Customer Relationships Management (CRM) system, http://www.salesforce.com/

[9] Cloud computing: http://www.springerlink.com

[10] Amazon EC2 and S3, Online at http://aws.amazon.com/

[11]Quality of service: http://osun.org/ http://www.sciencedirect.com/

[12] Salesforce.com, Inc., "Force.com platform," Retrieved Dec. 2009, from http://www.salesforce.com/tw/

Ch. Sai Krishna Manohar is pursuing the B.Tech degree in Information Technology at Tirumala Engineering College (JNTU-Kakinada) .He is a Certified Ethical Hacker (CEH) and also Certified Information Security Expert (CISE). He has already given so many presentations in various colleges and universities. Also he has been published number of technical papers at various Journals. His research interests include Network security, cloud computing, BIG DATA.