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

Computer Science and Engineeering

Elixir Comp. Sci. & Engg. 56 (2013) 13481-13484

ISSN: 2229-712X

Secure and Robust Cloud Storage with Cryptography and Access Control

R. Kalaichelvi[1] and L. Arockiam[2]

[1]Department of Computer Science, Karpagam University, Coimbatore, India.

[2]St. Joseph's College, Tiruchirappalli, India.

ARTICLE INFO

Article history:

Received: 17 February 2013;

Received in revised form:

11 March 2013;

Accepted: 12 March 2013;

Keywords

Authentication,
Cryptography,
Data security,
Encryption.

ABSTRACT

Cloud computing is a new evolving paradigm to a wide range of users like individuals, businesses and governments to provide resources in an on-demand environment. Enterprises store their incredible abundance of data on cloud to reduce data management cost. In addition, an emerging class of entrepreneurs is taking advantage of clouds as they might not have enough finance to purchase resources or ensure the necessary security. As the data is stored on cloud service providers' servers, confidentiality, authentication and access control are the most challenging factors in data security. Cloud providers should provide adequate security measures on their data and applications. Cryptography access control architecture overcomes the issue of data security in cloud environment. In this paper, we illustrate a secure and robust cloud storage architecture by combining cryptography and access control with two layered encryption.

1. Introduction

A. Cloud Computing

Cloud computing is a promising, evolving Internet computing of this era. It presents the users with a secure storage for storing the documents online wherein the users can take the benefit of privilege to access it remotely avoiding the usage of the data storage services. The companies which use the newly developed cloud computing model purchase the computing resources with the capabilities of scalability of expanding the resources, providing on-demand privilege with a little or no up-front IT infrastructure investment costs.

A new profitable way of delivering computing resources are done through cloud. It is a mixture of various computing entities, globally separated, but electronically connected. It is an Internet - based service delivery model. It offers services to markets like hospitals and business regimes. Cloud computing has taken IT to an upper level by giving people of the digital world to store information with bendable and measurable processing capability to cope up with the expanding need of demand and supply, whilst reducing capital expenditure. Cloud computing uses imaginary substructure and constructs a network, which can be used as the services in distributed computing, software services, internetworking, and internet services. It has exhibited enormous effort to empower fast, secure, trustable, integral, with a high performance, quantifiable, available data maintenance and security.

B. Service Models:

The deployment of the cloud computing services will vary based on the necessity of any business model once the cloud is formed. The basic service models [1] which can be deployed are as listed below:

Infrastructure as a Service (IaaS):

IaaS provides the customers the virtual devices that persuade the necessities on the needs of the customer services and the applications such as memory, CPU, OS and data space, reducing the expenses and the use of devoted systems. IaaS presents an intermediary policy to run subjective OS and software in case of scrupulous service constraints.

Platform as a Service (PaaS):

PaaS is an application platform wherein users can purchase access to the platform so that they can deploy their own softwares and the conventional applications with their services on the cloud. It is more economical, even though services need to be supported and managed.

PaaS distributes application development tools. Testing, collaborating, hosting, and managing applications are the services can be done by PaaS. It conceals the details of handling hardware. All support for the construction and distribution of web based applications are offered by PaaS online.

Software as a Service (SaaS):

For software operation in cloud system, SaaS is a prototype. The providers offer software to the clients through SaaS on demand. Users can buy the right to use and make use of an application or service that is hosted in the cloud. A standard example of this is Salesforce.com [12] in which the necessary knowledge for the interaction between the consumer and the service is organized as an element of the facility in the cloud.

C. Deployment Models

The cloud models [2] based on where they are deployed is divided into four types which can be explained as below:

Public Cloud:

This model is offered through the web applications or the website services online wherein sharing the hosting of information or the application is possible. A third party buys this kind of cloud model and the user can just use the services paying out a certain amount based on the efficacy.

Private Cloud:

Private cloud is mainly used for the internal utilization of any organization within its firewall, which is owned and managed by the company itself. The user working for that company only can make use of the resources available on the cloud which is bought by the owner. The user can make use of

Tele:
E-mail addresses: kalai_hasan@yahoo.com

the virtualized resources for the healthy management of the same.

Hybrid Cloud:

A hybrid model, as the name itself suggests is a combination of the public and private clouds. There are various internal as well as external suppliers of the cloud. The users use private or public cloud depending on the criticality of the data transfer. Private cloud is used mainly when the crucial, confidential information needs to be transferred whereas the public cloud is used mainly to handle large transactions smoothly at peak timings.

Community Cloud:

This is a kind of substructure which can be allocated to various organizations, which is normally delivered on private cloud. The advantage of using a community cloud is that the supplier can have as many numbers of clients as he gets and can charge for organizations individually.

II Motivation And Objectives

A. Data Storage in Cloud

Cloud computing has emerged as feasible and readily available platform to a wide range of users like individuals, businesses and governments. Nowadays most of the enterprises store their sensitive and confidential data on cloud to reduce the investment on new software, hardware and storage medium. Also startups use clouds as they might not have enough finance to purchase resources or ensure the necessary security. The Data Owners (DO) of enterprises or startups use the advantage of pay-per-use feature of cloud. Cloud storage is a key for backup outsourcing of any enterprises or government agencies. Traditionally, the DOs archive their data on their own data centers. But the investment of data management is very expensive as their data volume is huge. Significantly they are migrating to cloud for storing their data. Since the backup is on cloud, universal access of data is possible. This reduces the capital expenditure on resources. It nullifies the storage management problem of DOs. The users can access data from any location. Hence cloud storage is more versatile and suitable for well-established businesses.

There are various types of cloud storage systems [6]. Some of them store email messages, some for storing pictures, while others store all types of data in their data pool. Hundreds of servers are used by a cloud service provider. Most of the enterprises use the cloud for archiving their data. When a data owner stores data in cloud, it is stored in more than one server. Hence users can access their data at any time from the cloud even though if there is a problem in one server. A several commercial cloud models are developed by Cloud Service Providers (CSP) like Microsoft Azure, Amazon's EC2 and S3, Dropbox, and icloud [3,4] etc. As these providers offer storage as a service, the models are defined as "Storage as a Service" [3].

The Table 1 shows the popular cloud storage providers [7].

Table 1. Popular Cloud Storage Providers

justcloud.com	mozy
Zipcloud	backupGenie
mypcbackup.com	dropbox
sos onlinebackup	box
sugarsync - 128 bit AES encrypted format	Crahsplan
google drive	apple's icloud

B. Data Security

Though Cloud computing has its own advantages in storing a huge amount of data, it also faces data security challenges. Some of the challenging factors in data security include confidentiality, authentication and access control. As the service providers can get access to the data stored in their servers, if the service providers misuse the data for their gain, then it would be a great loss to the data owners.

As data owners are using virtual environment to store their data on clouds, data security is most vital factor to be considered. To ensure security, cloud providers, data owners and users should take proactive measures. The entities of cloud can be public sources or businesses which process sensitive information. So the degree of security also varies with types of cloud entities. The data from public sources may not require a high degree of security. On the other hand, business handling sensitive data viz banks, other financial establishments or governments require a high level of security for their sensitive data on cloud. In this scenario, cloud providers should provide adequate security measures on their data and applications.

The degree of security varies user by user; cybercriminals can target weaker entity/entities of a cloud provider which have lack of security in them. Other entities which reside in the provider may also be compromised. The nature of cloud architecture provides chance for malicious attacks to hundreds of sites by cybercriminals.

C. Data's CIA

Three pillars of cloud security requirements are confidentiality, integrity and availability (CIA) [8]. If these requirements are achieved by any cloud community then it is a highly secured system. But in reality, achieving the CIA requirements is difficult.

Identifying policies, laws and standards helps to ensure data's CIA. The cloud community should establish effective policies and governance to implement adequate security methods. The US National Institute of Standards and Technology (NIST) promotes such policies [8]. Cloud community must make an effort to develop a policy of self-regulation to ensure security in addition to NIST's support. Cloud security needs can be addressed by adopting NIST's policies and the best practices of cloud communities in achieving CIA's of data.

To promote confidentiality, integrity and availability (CIA) of data, the cloud provider should have an appropriate encryption plan to store data. Also a rigorous access control mechanisms should be implemented to avert any unauthorized users accessing data. To achieve a significant role of cloud computing security, we must build up a security model that supports CIA with the adoption of universal standards.

III Access Control Architecture

A. Authentication and Authorization

There is a risk in outsourcing data if cloud service provider may be vulnerable to attack. To ensure the data is confidential as well as available to only legal users, authentication [13] and authorization [14] mechanisms get involved in cloud storage. Authentication method is used to make out the legal users while, authorization determines the privileges of users.

Accessing system in cloud environment by authentication is a method of guaranteeing the users who are authorized users. The potency of an authentication mechanism can be assessed on many things it depends on what the user knows, possess and what the user has. Authentication is a process of verifying and validating the user’s possession or the testimonial. There are many schemes are projected for user authentication like textual

password, graphical password, one time password, finger print, retina scan etc.

Authorization is the process of allocating the levels of access to services and resources by clients. It is the process of providing clients permission to access the services based on defined access policies from cloud services providers. Access control [5] of services relies on authentication and authorization mechanisms in cloud paradigm to avoid illegitimate users from accessing secured resources.

The Figure 1. depicts the conceptual framework of authentication and authorization involved in cloud computing. When a cloud user requests a service from CSP using his identity as an authentication tool, CSP verifies user's credentials as well as his rights on resources. After verification, if the user is an authorized user, CSP provides the respective services.

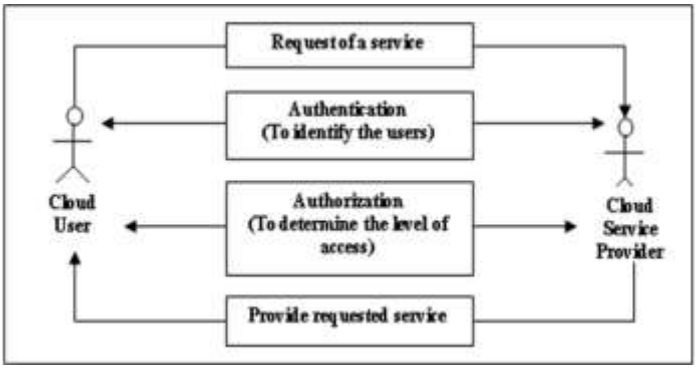

Figure 1. Conceptual Framework of Authentication and Authorization in Cloud Computing

B. Traditional Access Control Architecture

In recent years, individuals and big businesses adopt data storage in cloud commonly, where DO stores their data on cloud. As cloud may not be a trusted domain, there can be risks of confidentiality and privacy breaks. In traditional access control architecture, data is stored in cloud. The accessibility of data by the user is controlled by the cloud provider. The cloud server is responsible for defining and implementing access control policies. But as it is a third party to the DO, it may not be a trusted domain having control on data. In the proposed novel model, the cloud provider is no longer in charge of validating access requests or no control on access control policies. The access control policy is defined and modified only by the data owner.

In traditional architecture [9], as shown in Figure 2 Data Owner (DO) stores data in Cloud Service Provider (CSP). Cloud Service Provider is full charge of managing access control policy. When an authorized user (U) requires data, user retrieves the data from CSP. The transmission of data is controlled by CSP. But as the data owner and the cloud service provider are two different entities, CSP may fall outside the trusted domain.

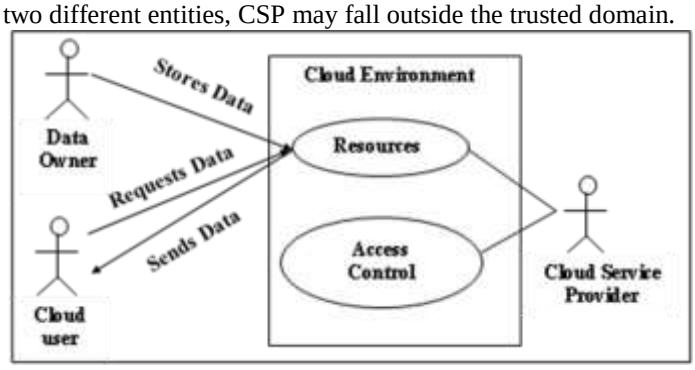

Figure 2. Traditional Access Control Architecture

C. Cryptography Access Control Architecture

Cryptography access control architecture [10, 11] overcomes the above issue of data security in cloud environment. Cryptography technique shown in Figure 3 is used to ensure data security in cloud. DO stores data in CSP in an encrypted form in this cryptography architecture. Risk of loss of sensitive information can be reduced by encryption. Hence CSP does not even know about the data which is stored by DO. The validation of user's identity and the level of access are controlled by DO. When a user requires data, he requests DO. DO sends required keys and certificates to the user, upon his request. Here authorization and encryption are merged to provide protection to the data on cloud. By using this certificate user requests CSP for accessing data which is stored by DO. After the verification of his credentials CSP allows users to access the encrypted data. Then the user decrypts the data by the key that is sent by DO. The assumption in this architecture is that all users have same rights to access complete data. In this scenario, one distinct key is used in encrypting complete data. But in reality different users might need different segments of data. Also whenever there is a need in accessing data by the user, DO gets involved. This mechanism requires the DO should be available all the time when there is a transmission of data.

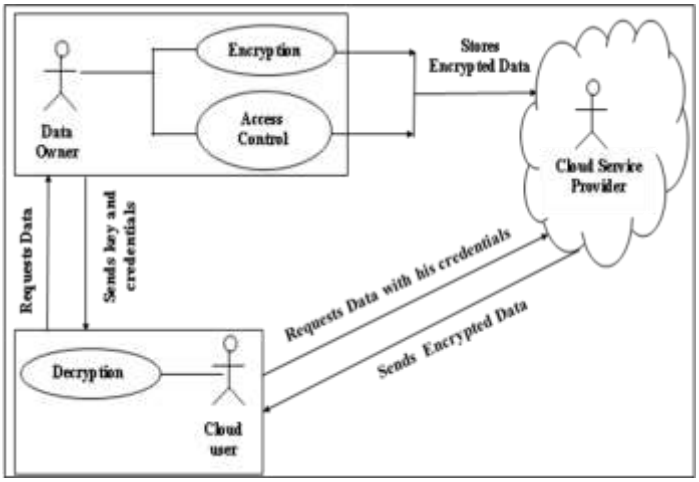

Figure 3. *Cryptography Access Control Architecture*

D. Secure and Robust Cryptography Architecture

Nevertheless a single key for encrypting the complete data is not enough when users need different data at different time. In this scenario, a multi key approach is the robust and efficient solution to extract plain text from encrypted data. To provide an adequate protection from malicious, unauthorized users the DO should give an ample attention to two features viz storage of encrypted data and storage and management of access policies.

To overcome the issues mentioned above, we propose a secure and robust cryptography architecture. The Figure 4 illustrates the secure, robust cryptography architecture. There are two layers of encryption adopted in this new model. Firstly DO encrypts data before it transmits to CSP. Secondly the CSP encrypts the encrypted data as a second protection. When a user needs to access the data, he receives two secret keys viz one key from the DO and other key from CSP. Former key is to decode the encryption performed by DO and the later is to access data where the encryption done by CSP. And then the multi key approach takes place to have a control on access policy. DO creates a list of keys for different data. DO sends a secret key as well as a set of keys for accessing data to the user when he requests data. The secret key is used to authorize to access the

set of keys for accessing data. The user should be able to decrypt the data using the set of keys sent by the data owner.

Combination of access control and cryptography approach with multiple key is a better choice to ensure confidentiality of data stored on cloud. The traditional additional authorization layer with cryptography conquers the leakage of sensitive information on cloud.

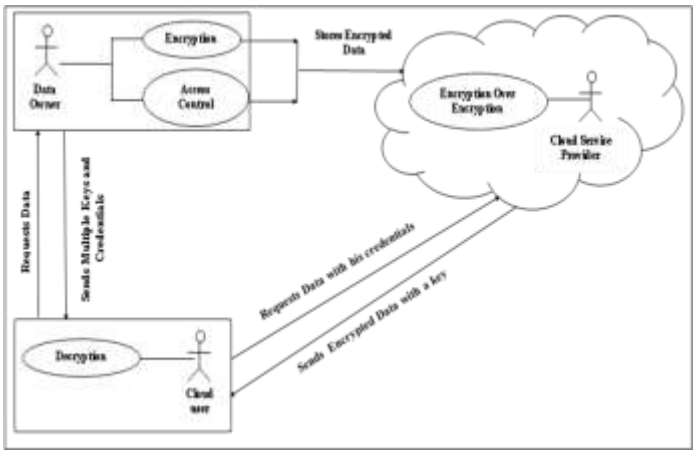

Figure 4. ***Secure and Robust Cryptography Architecture***

IV Conclusion

A demanding research area in cloud computing is data security. This paper addressed the various problems and issues involved in cloud storage when implementing access control by CSP. It also explored the issues and impacts that arise when a single key encrypts complete data in cryptography architecture. It then proposed a new architecture to support data's confidentiality, integrity and availability by combining cryptography with access control using multi key approach. Moreover, it described how authorization layer guarantees the appropriate data access to cloud users. The proposed approach is the beginning of a long line of different access control policies. Future extensions will include key management and distribution scenarios, and the efficient execution of queries.

References

[1] Meiko Jensen et al., "On Technical Security Issues in Cloud Computing", *IEEE International Conference on Cloud Computing*, Bangalore, pp 109-116, 2009.

[2] R. Kalaichelvi et al., "Research Challenges and Security Issues in Cloud Computing", *International Journal of Computational Intelligence and Information Security*, Vol. 3, No. 3 pp 42-48, March 2012.

[3] Chittaranjan Hota et al., "Capability based cryptographic data access control in cloud computing", *International Journal of Advanced Networking and Applications*, vol 01, issue. 1, pp 1152 - 1161, 2011.

[4] Sonam Chugh et al., " Access Control Based DAta Security in Cloud Computing", *International journal of Engineering Research and Applications*, vol. 2, issue 3, pp 2589-2593, May-June 2012.

[5] Yang Tang et al. "Secure Overlay Cloud Storage with Access Control and Assured Deletion", *IEEE Transactions on dependable and secure computing, published by IEEE Computer Society'* vol 9, no. 6, dec 2012.

[6] Cloud Storage on the web at http://computer.howstuffworks.com/cloud-computing/cloud-storage1.htm.

[7] Top 10 best online backup at http://www.thetop10bestonlinebackup.com/.

[8] Kaufman et al. "Data Security in the world of cloud computing", *Security and Privacy, IEEE*, vol. 7, issue 4, pp 61-64, Aug 2009

[9] Sabrina et al. "A Data Outsourcing Architecture Combining Cryptography and Access Control", *CSAW'07 ACM Workshop on Computer Security Architecture*, USA, pp 63-69, Nov 2007.

[10] S. Yu, C. Wang et al. "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", *Porc. IEEE INFOCOM*, San Diego, CA, pp 1-9, 2010.

[11] W. Wang et al. "Secure and efficient access to outsourced data", *ACM Cloud Computing Security Workshop 2009*, Chicago, USA, pp 55-65, 2009.

[12] Salesforce.com cloud computing company on the web at http://www.salesforce.com/cloudcomputing/.

[13] Hongwei Li et al., "Identity-Based Authentication for Cloud Computing", *CloudCom 2009, Springer-Verlag Berlin Heidelberg*, pp 157-166, 2009.

[14] Hongxin Hu et al. "Construction Authorization Systems Using Assurance Management Framework", IEEE Transactions on Systems, Man, and Cybernetics—part c: applications and reviews, vol. 40, no. 4, pp 396-405, july 2010

Authors Profile

Ms. R. Kalaichelvi is working as an Asst. Professor in AMA International University, Kingdom of Bahrain. She is currently pursuing her research in Karpagam University, Coimbatore, India. She has published 6 research articles in the International / National Journals. Her areas of research interests are in Cloud Computing, Data Security, Cryptography and Data mining.

Dr. L. Arockiam is working as an Associate Professor in St.Joseph's College, India. He has published 102 research articles in the International / National Conferences and Journals. He has also authored two books: "Success through Soft Skills" and "Research in a Nutshell. His areas of research interests are: Software Measurement, Cloud Computing, Cognitive aspects in Programming, Web Service, Mobile Networks and Data mining.