Achieving Secure, Scalable and Fine Grained Data Access Control in Cloud Computing

Yallamanda Challa
Hindustan University
Chennai, India
challa.ynaidu@gmail.com

ABSTRACT: *Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. This paper proposed some services for data security and access control when users outsource sensitive data for sharing on cloud servers. This paper addresses this challenging open issue by, on one hand, 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 un trusted cloud servers without disclosing the underlying data contents.*

Our proposed scheme enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability and achieves fine - graininess, scalability and data confidentiality for data access control in cloud computing. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

Keywords: Proxy Re-Encryption, Proxy Re-Encryption, Data Access, Data Security, Cloud servers

Received: 29 March 2012, Revised 31 May 2012, Accepted 4 June 2012

1. Introduction

Cloud computing is also facing many challenges that, if not well resolved, may impede its fast growth. Data security, as it exists in many other applications, is among these challenges that would raise great concerns from users when they store sensitive information on cloud servers. These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users.

Data confidential against cloud servers is hence frequently desired when users outsource data for storage in the cloud. In some practical application systems, data confidentiality is not only a security/privacy issue, but also of juristic concerns. For example, in healthcare application scenarios use and disclosure of protected health information (PHI) should meet the requirements of Health Insurance Portability and Accountability Act (HIPAA), and keeping user data confidential against the storage servers is not just an option, but a requirement. Furthermore, we observe that there are also cases in which cloud users themselves are content Providers. They publish data on cloud servers for sharing and need fine-grained data access control in terms of which user (data consumer) has the access privilege to which types of data. In the healthcare case, for example, a medical center would be the data owner who stores millions of healthcare records in the cloud. It would allow data consumers such as doctors, patients, researchers and etc, to access various types of healthcare records under policies admitted by HIPAA. To enforce these access policies, the data owners on one hand would like to take advantage of the abundant resources that the cloud provides for efficiency and economy; on the other hand, they may want to keep the data contents confidential against cloud servers.

Cloud computing is also facing many challenges that, if not well resolved, may impede its fast growth. Data security, as it exists in many other applications, is among these challenges that would raise great concerns from users when they store sensitive information on cloud servers. These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users.

Data confidential against cloud servers is hence frequently desired when users outsource data for storage in the cloud. In some practical application systems, data confidentiality is not only a security/privacy issue, but also of juristic concerns. For example, in healthcare application scenarios use and disclosure of protected health information (PHI) should meet the requirements of Health Insurance Portability and Accountability Act (HIPAA), and keeping user data confidential against the storage servers is not just an option, but a requirement.

2. Existing System

Our existing solution applies cryptographic methods by disclosing data decryption keys only to authorized users. These solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well.

In the existing work owner only responsible for distribution of keys and distribution of data to the particular client, so he is unable to concentrate on both of the work. Therefore client request not fully satisfied in concerned time. Fine grained data also not properly accessed.

Limitation: (i) Data management when fine grained data access control is desired,and thus do not scale well. (ii) Heavy computation overhead on the data owner for key distribution and data accessing.

3. Proposed System

In order to achieve secure, scalable and fine-grained access control on outsourced data in the cloud,we utilize and uniquely combine the following three advanced cryptographic techniques: (i) Key Policy Attribute-Based Encryption (KP-ABE). (ii) Proxy Re-Encryption (PRE). (iii) Lazy re-encryption.

Advantages:

- Low initial capital investment
- Shorter start-up time for new services
- Lower maintenance and operation costs
- Higher utilization through virtualization
- Easier disaster recovery

4. Literature Servey

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps are to determine which operating system and language can be used for developing the tool.

Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

3.1 Demographics

F5 Networks spoke with 250 companies. All companies included in the survey had at least 2,500 employees worldwide, with a median of 75,000 employees.

37 percent of respondents were IT managers. 24 percent were VPs, 23 percent were IT directors, and 16 percent were SVPs. No CIOs were included in this study Of all respondents, 46 percent manage an IT department, 41 percent work in an IT department, and the IT department reports to13 percent.

3.2 Defining the cloud

F5 Networks also conducted a focus group of IT managers, network architects andcloud service providers in order to establish a firm definition of cloud computing. Focus group participants debated the merits of each definition in the survey, and agreed upon the following as a standard definition for cloud computing.

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "*cloud* " that supports them. Furthermore, cloud computing employs a model for enabling available, convenient and on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

3.3 The Cloud Is More Than SAAS

IT managers commonly equate Cloud Computing with Software-as-a-Service(SaaS). Although SaaS is an important element of cloud computing, IT managers do not see it as the most important element.

Three-fourths of respondents reported that Platform-as-a-Service (PaaS) is usually or always included in the cloud. Additionally, two-thirds said Infrastructure-as-a-Service (IaaS) is usually or always included in the cloud. By way of comparison, three-fifths said SaaS was usually or always included in a cloud deployment.

3.4 Core Cloud Technologies

As budgets for cloud computing increase, IT managers are examining critical technologies for building the infrastructure behind the cloud. 90 percent of respondents named access control as somewhat/very important for building the cloud. An additional 89 percent listed network security as a core technology. 88 percent of respondents listed both server and storage virtualization as essential technologies in the cloud.

3.5 Influencers Go Beyond IT

Though IT is intrinsically a part of cloud computing, it is not the only influencer over an organization's cloud computing policies. Survey respondents claimed that IT generally controls the cloud computing budget (64 percent compared to the 13 percent each held by application development and network architects). According to respondents, the top influencers for public clouds include IT (45 percent), application development (41 percent) and LOB business stakeholders (41 percent).

On a similar note, respondents claimed the top three influencers in the implementation process for private clouds are IT (45 percent), LOB business unit stakeholders (36 percent) and application development teams (24 percent).

5. Modul Description and Assumptions

5.1 System Models

Similar to, we assume that the system is composed of the following parties: the Data Owner, many Data Consumers, many Cloud Servers, and a Third Party Auditor if necessary. To access data files shared by the data owner, Data Consumers,or users for brevity, download data files of their interest from Cloud Servers and then decrypt. Neither the data owner nor users will be always online. They come online just on the necessity basis.

For simplicity, we assume that the only access privilege for users is data file reading. Extending our proposed scheme to support data file writing is trivial by asking the data writer to sign the new data file on each update as does. From now on, we will also call data files by files for brevity. Cloud Servers are always online and operated by the Cloud Service Provider (CSP).

They are assumed to have abundant storage capacity and computation power. The Third Party Auditor is also an online party which is used for auditing every file access event. In addition, we also assume that the data owner can not only store data files but also run his own code on Cloud Servers to manage his data files. This assumption coincides with the unified ontology of cloud computing.

5.2 Security Models

In this work, we just consider Honest but Curious Cloud Servers as does. That is to say, Cloud Servers will follow our proposed protocol in general, but try to find out as much secret information as possible based on their inputs. More specifically, we assume Cloud Servers are more interested in file contents and user access privilege information than other secret information. Cloud Servers might collude with a small number of malicious users for the purpose of harvesting file contents when it is highly beneficial.

Communication channel between the data owner/users and Cloud Servers are assumed to be secured under existing security protocols such as SSL. Users would try to access files either within or outside the scope of their access privileges. To achieve this goal, unauthorized users may work independently or cooperatively. In addition, each party is preloaded with a public/private key pair and the public key can be easily which is used obtained by other parties when necessary.

5.3 Design Goals

Our main design goal is to help the data owner achieve fine-grained access control on files stored by Cloud Servers. Specifically, we want to enable the data owner to enforce a unique access structure on each user, which precisely designates the set of files that the user is allowed to access.

We also want to prevent Cloud Servers from being able to learn both the data file contents and user access privilege information. In addition,the proposed scheme should be able to achieve security goals like user accountability and support basi coperations such as user grant/revocation as a generalone-to-many communication system would require. All these design goals should be achieved efficiently in the sense that the system is scalable.

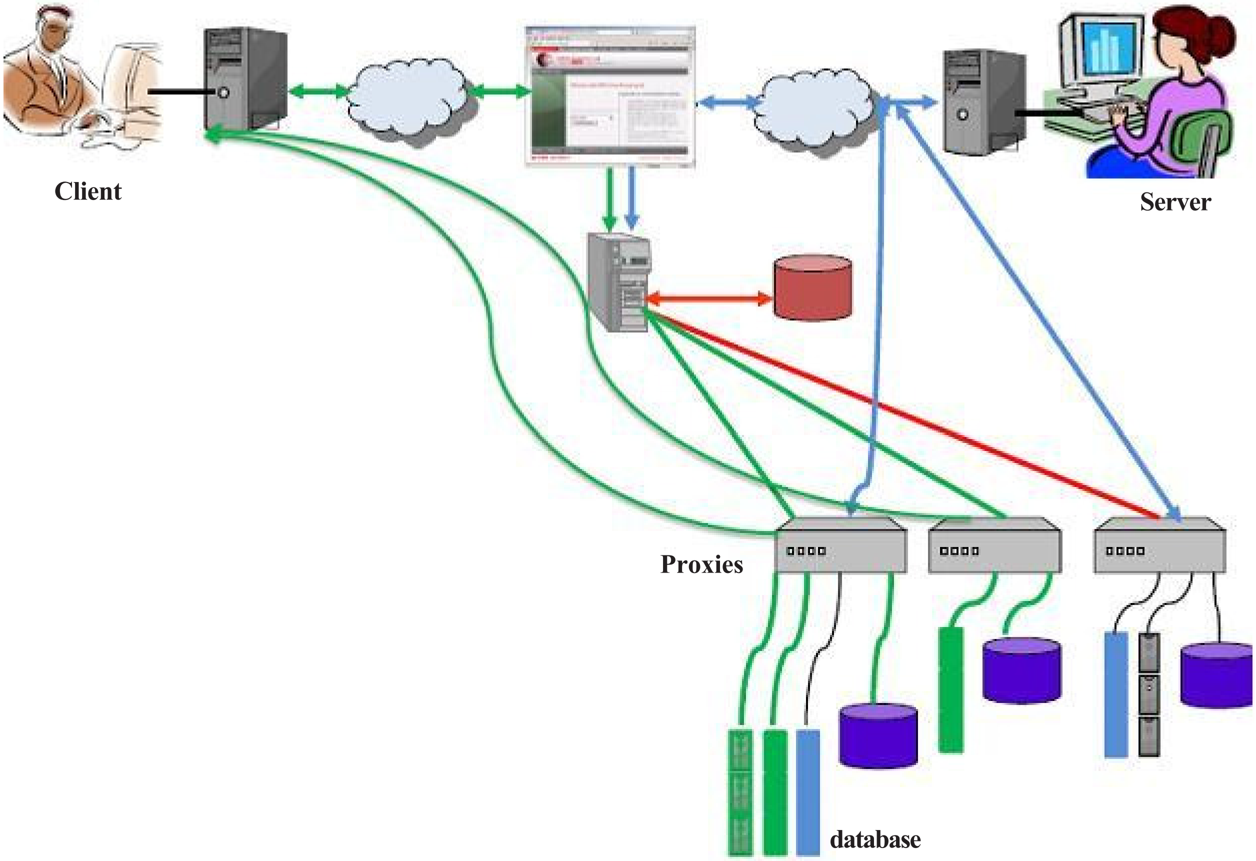

Figure 1. System archicture

In our proposed scheme, we exploit the technique of hybrid encryption to protect data files i.e., we encrypt data files using symmetric DEKs and encrypt DEKs with KPABE. Using KP-ABE, we are able to immediately enjoy fine-grained data access control and efficient operations such as file creation/deletion and new user grant.To resolve the challenging issue of user revocation, we combine the technique of proxy re-encryption with KP-ABE and delegate most of the burdensome computational task to Cloud Servers. We achieve this by letting Cloud Servers keep a partial copy of each user's secret key, i.e., secret key components of all but one (dummy) attributes. When the data owner redefines a certain set of attributes for the purpose of user revocation, he also generates corresponding proxy re-encryption keys and sends them to Cloud Servers. Cloud Servers, given these proxy re-encryption keys, can update user secret key components and re-encrypt data files accordingly without knowing the underlying plaintexts of data files. This enhancement releases the data owner from the possible huge computation overhead on user revocation. The data owner also does not need to always stay online since Cloud Servers will take over the burdensome task after having obtained the PRE keys. To further save computation overhead of Cloud Servers on user revocation, we use the technique of lazy reencryption and enable Cloud Servers to "*aggregate*" multiple successive secret key update/file reencryption operations into one, and thus statistically save the computation overhead.

6. Conclusion

Context is to achieve finegrainedness, data confidentiality, and scalability simultaneously, which is not provided by current work. In this paper we propose a scheme to achieve this goal by exploiting KP-ABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption. Moreover, our proposed scheme can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved. Formal security proofs show that our proposed scheme is secureunder standard cryptographic models.

7. Future Enchancement

This paper aims at fine-grained data access control in cloud computing. One challenge in this

References

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., Zaharia, M. (2009). Above the clouds: A berkeley view of cloud computing, University of California, Berkeley, Tech. Rep. USB-EECS-2009-28.

[2] McDaniel, P. D., Prakash, A. (2002). Methods and limitations of security policy reconciliation, *In*: Proc. of SP'02.

[3] Yu, T., Winslett, M.(2003). A unified scheme for resource protection in automated trust negotiation, *In*: Proc. of SP'03.

[4] Li, J., Li, N., Winsborough, W. H. (2005). Automated trust negotiation using cryptographic credentials, *In*: Proc. of CCS'05.

[5] Anderson, J. Computer Security Technology Planning Study, Air Force Electronic Systems Division, Report ESD-TR-73-51, and http://seclab.cs.ucdavis.edu/projects/history/.

[6] Goh, E. ,Shacham, H., Modadugu, N., Boneh, D. Sirius: Securing remote untrusted storage, *In*: Proc of NDSS'03.

[7] Ateniese, G., Fu, K., Green, M., Hohenberger, S. (2005). Improved proxy re-encryption schemes with applications to secure distributed storage, *In*: Proc. Of NDSS'05.