A Third Party Auditor Based Technique for Cloud Security

Dinesh Kumar Bhayal[1] Prof. Gajendra Singh[2]
[1,2]SSSIST, Sehore (MP)

Abstract-- Cloud security means providing security to users data. There are so many methods for doing this task. They all have their merits and demerits. To ensure the security of users' data in the cloud, we propose an effective, scalable and flexible cryptography based scheme. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against malicious data modification attack, The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

I. INTRODUCTION

CLOUD computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, utility computing, and service-oriented architecture. In the last several years, cloud computing has emerged as one of the most influential paradigms in the IT industry, and has attracted extensive attention from both academia and industry. Cloud computing holds the promise of providing computing as the fifth utility [1] after the other four utilities (water, gas, electricity, and telephone). The benefits of cloud computing include reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility, immediate time to market, and so on. Different service-oriented cloud computing models have been proposed, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Numerous commercial cloud computing systems have been built at different levels, e.g., Amazon's EC2 [2], Amazon's S3 [3], and IBM's Blue Cloud [4] are IaaS systems, while Google App Engine [5] and Yahoo Pig are representative PaaS systems, and Google's Apps [6] and Salesforce's Customer Relation Management (CRM) System [7] belong to SaaS systems. With these cloud computing systems, on one hand, enterprise users no longer need to invest in hardware/software systems or hire IT professionals to maintain these IT systems, thus they save cost on IT infrastructure and human resources; on the other hand, computing utilities provided by cloud computing are being offered at a relatively low price in a pay-as-you-use style. For example, Amazon's S3 data storage service with 99.99% durability charges only $0.06 to $0.15 per gigabyte-month, while traditional storage cost ranges from $1.00 to $3.50 per gigabyte-month according to Zetta Inc. [8]. Although the great benefits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security problems in cloud computing become serious obstacles which, without being appropriately addressed, will prevent cloud computing's extensive applications and usage in the future. One of the prominent security concerns is data security and privacy in cloud computing due to its Internet- based data storage and management. In cloud computing, users have to give up their data to the cloud service provider for storage and business operations, while the cloud service provider is usually a commercial enterprise which cannot be totally trusted. Data represents an extremely important asset for any organization, and enterprise users will face serious consequences if its confidential data is disclosed to their business competitors or the public. Thus, cloud users in the first place want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors. This is the first data security requirement. Data confidentiality is not the only security requirement. Flexible and fine-grained access control is also strongly desired in the service-oriented cloud computing model. A health-care information system on a cloud is required to restrict access of protected medical records to eligible doctors and a customer relation management system running on a cloud may allow access of customer information to high-level executives of the company only. In these cases, access control of sensitive data is either required by legislation (e.g., HIPAA) or company regulations.

II. PROPOSED SYSTEM

A. Proposed System:

In our proposed model, the client or user interacts with the third party auditor. The third party auditor is an authorized person appointed by the owner of the cloud. In our model, both data and auditor are present at the cloud servers site.It is responsible for performing functions at all the three layers.

The first layer is USER AUTHENTICATION
The second layer is DATA ENCRYPTION AND DATA PROTECTION
The third layer is DATA DECRYPTION

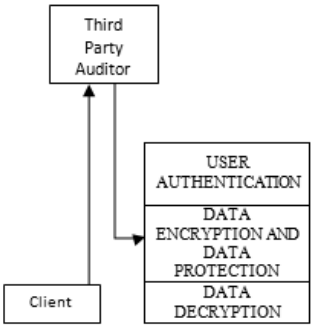

Fig. 1: Proposed Model

B. Key Structure

We use a recursive set based key structure as in [9] where each element of the set is either a set or an element corresponding to an attribute. The *depth* of the key structure is the level of recursions in the recursive set, similar to definition of depth for a tree. For a key structure with depth 2, members of the set at depth 1 can either be attribute elements or sets but members of a set at depth 2 may only be attribute elements.

C. Access Structure

In our scheme, we use the same tree access structure as in [9]. In the tree access structure, leaf nodes are attributes and nonleaf nodes are threshold gates. Each nonleaf node is defined by its children and a threshold value. Let denote the number of children and the threshold value of node.

III. CONCLUSION

In this paper, we proposed a new method for providing security to users data in cloud computing environment. Our proposed model is efficient, scalable, and flexible. Our model adopts hierarchical structure, therefore it is easily scalable. As multiple auditors are involved in handling users data.

REFERENCES

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput. Syst., vol. 25, pp. 599–616, 2009.
[2] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/
[3] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws. com/
[4] R. Martin, "IBM brings cloud computing to earth with massive new data centers," InformationWeek Aug. 2008 [Online]. Available: http:// www.informationweek.com/news/hardware/data_centers/209901523
[5] Google App Engine [Online]. Available: http://code.google.com/appengine/
[6] K. Barlow and J. Lane, "Like technology from an advanced alien culture: Google apps for education at ASU," in Proc. ACM SIGUCCSUser Services Conf., Orlando, FL, 2007.
[7] B. Barbara, "Salesforce.com: Raising the level of networking," Inf.Today, vol. 27, pp. 45–45, 2010.
[8] J. Bell, Hosting EnterpriseData in the Cloud—Part 9: InvestmentValue Zetta, Tech. Rep., 2010.
[9] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

