Cloud computing security: A phased approach

Dushyant Singh
M.Tech Student, SKIT, Jaipur

Vipin Jain
Sr. Lecturer, SKIT, Jaipur

Subham Kumar Gupta
Lecturer, SKIT, Jaipur

Abstract - Cloud computing has been considered as the future of IT Enterprise. In contrast to traditional solutions in which the IT services are under proper physical, logical and personnel controls, It moves all the computing resources to the centralized large data centres, so users can enjoy scalable services on demand. Especially small and medium-size enterprises can manage their projects by using cloud-based services and also able to achieve productivity enhancement with limited budgets. But, apart from all of these benefits, it may not be fully trustworthy. Cloud Computing do not keep data on the user's system, so there is a need of data security. The user pays more & more attention about data security due to this off-side storage of data on cloud computing. In order to retain confidentiality of data against un-trusted cloud service providers, There are so many approaches. All modern cloud service providers solve this problem by encryption and decryption techniques. They all have their merits and demerits. In this paper, we investigate the basic problem of cloud computing security. We have also proposed a survey of various models for cloud security. 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 achieves scalability as well as flexibility due to its hierarchical structure.

Keywords: Cloud Computing; CSP; ASBE, HASBE.

I. INTRODUCTION

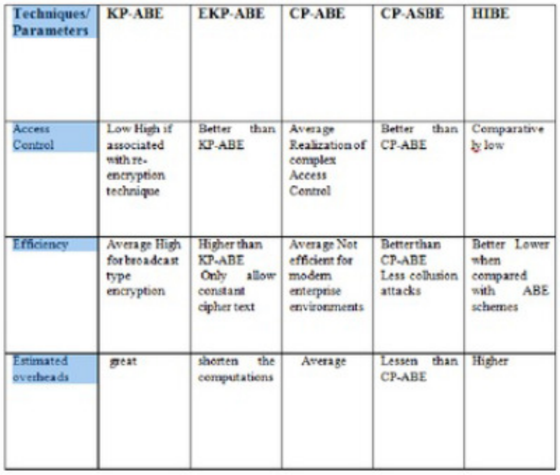
CLOUD computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, utility computing and service-oriented architecture. In the last several years, cloud computing has emerged as one of the most influential paradigms in the IT industry, and has attracted extensive 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 less costs and capital expenditures, more 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 Due to these cloud computing systems, enterprise users no longer need to invest in hardware & software systems and to hire IT professionals to maintain these IT systems, so they save cost on IT infrastructure and human resources; also, 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 service for data storage 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 cloud computing paradigm offers great benefits for IT Enterprises, academic researchers, and potential users, but we cannot neglect security problems in cloud computing. Most prominent security concern is data security and privacy in cloud computing due to its Off-site data storage and management. The cloud service provider is usually a commercial enterprise which cannot be totally trusted in case of storage of sensitive user's data. Data is an important asset for any organization, and in case of disclose of that data to their business competitors or the public, enterprise will face serious consequences. So cloud users want to make sure that their data remains confidential to cloud provider and every other entity. This is the first & most data security requirement. Flexibility and fine-grained access control are other important requirements in case of service-oriented cloud computing model.

II. Related Work

In cloud computing, there are different existing schemes that provide security, data confidentiality and access control. Users need to share sensitive objects with others based on the recipient's ability to satisfy a policy in distributed systems. One of the encryption schemes is Attribute Based Encryption (ABE) which is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CP-ABE) scheme. In KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. Only the keys associated with the policy that is satisfied by the attributes associating the data can decrypt the data. In CP-ABE schemes, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data.

Table I Comparison of Different Encryption Schemes



Techniques/ Parameters	KP-ABE	EKP-ABE	CP-ABE	CP-ASBE	HIBE
Access Control	Low High if associated with re-encryption technique	Better than KP-ABE	Average Realization of complex Access Control	Better than CP-ABE	Comparatively low
Efficiency	Average High for broadcast type encryption	Higher than KP-ABE Only allow constant cipher text	Average Not efficient for modern enterprise environments	Betterthan CP-ABE Less collusion attacks	Better Lower when compared with ABE schemes
Estimated overheads	great	shorten the computations	Average	Lessen than CP-ABE	Higher

III.Problem Identification

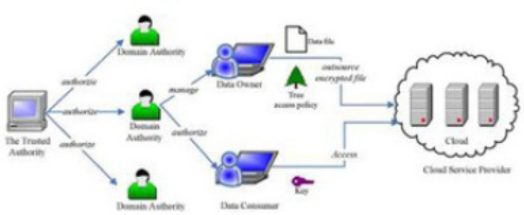


Fig. 1 Previous Model

3.1 Disadvantages of Existing System-

3.1.1 Software update/patches- It could change security settings, assigning privileges too low, or even more alarmingly too high allowing access to your data by other parties.

3.1.2 Security concerns- Experts claim that their clouds are 100% secure - but it will not be their head on the block when things go awry. It's often stated that cloud computing security is better than most enterprises. Also, you cannot decide which data to handle in the cloud and which to keep to internal systems. once decided, keeping it secure could well be a full-time task.

*3.1.3 Control-*Your data/system is controlled by third-party. Data once in the cloud always in the cloud! You cannot be sure that once you delete data from your cloud account will not exist anymore.

Although the present model overcomes the limitations of the third party auditor based scheme. But it follows a very complex hierarchical structure. We can propose a new model which combines the benefits of both present HASBE model and the third party auditor based model.

IV. 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 server 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

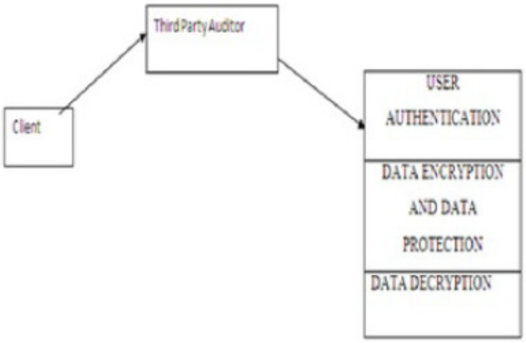


Fig. 2 Proposed Model

4.1 Advantages of Proposed Model:

4.1.1 Computational Overhead:

In our proposed scheme, the third party auditor and users data is on same site. So the time required for the authentication purpose and data encryption and decryption is less in comparison to previous schemes. In previous schemes, the data and the third party auditor were on separate site. It is clear that in that case the time required for authentication will be more.

4.1.2 Authentication Data Security:

In our proposed scheme, the authentication module is playing an intermediates role. Neither the cloud service provider nor the user of the data is able to access the authentication data from it.

4.1.3 Scalability:

We extend HASBE with a hierarchical structure to effectively delegate the trusted authority’s private attribute key generation operation to lower-level third party auditor. By doing so, the workload of the trusted root authority is shifted to lower-level domain authorities, which can provide attribute key generations for end users. Thus, this hierarchical structure achieves great scalability.

V. RESULT

5.1 Security:

We have proposed an enhancement in the existing model. In our enhanced model, the cloud server provider is authorized to store data owners encrypted data. But the cloud server provider in not authorized to store the data owners decryption key. In this way the cloud server provider is capable of accessing the data owners encrypted data. But he is not capable enough of decrypting the owners data. In this way the security of owners data is increased to a greater extent.

5.2 Scalability: We extend ASBE with a hierarchical structure to effectively delegate the trusted authority's private attribute key generation operation to lower-level domain authorities. By doing so, the workload of the trusted root authority is shifted to lower-level domain authorities, which can provide attribute key generations for end users. Thus, this hierarchical structure achieves great scalability. Yu *et al.*'s scheme, however, only has one authority to deal with key generation, which is not scalable for large-scale cloud computing applications.
5.3 Flexibility: Compared with Yu *et al.*'s scheme, new scheme organizes user attributes into a recursive set structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. So new scheme can support compound attributes and multiple numerical assignments for a given attribute conveniently.
Fine-grained access control: our scheme can easily achieve fine-grained access control. A data owner can define and enforce expressive and flexible access policy for data files as the scheme in [17].
5.4 Efficient User Revocation: To deal with user revocation in cloud computing, we add an attribute to each user's key and employ multiple value assignments for this attribute. So we can update user's key by simply adding a new expiration value to the existing key. We just require a domain authority to maintain some state information of the user keys and avoid the need to generate and distribute new keys on a frequent basis, which makes our scheme more efficient than existing schemes.
5.5 Expressiveness: In new scheme, a user's key is associated with a set of attributes, so new scheme is conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC) [18]. Thus, it is more natural to apply new scheme, instead of KP-ABE, to enforce access control.

VI. Conclusion

In this paper, we introduced the new scheme for realizing scalable, flexible, and fine-grained access control in cloud computing. The new scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. New scheme not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes. We formally proved the security of new scheme based on the security of CP-ABE.. Finally, we implemented the proposed scheme, and conducted comprehensive performance analysis and evaluation, which showed its efficiency and advantages over existing schemes.

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] A. Ross, "Technical perspective: A chilly sense of security," *Commun.ACM*, vol. 52, pp. 90–90, 2009.

[10] D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.

[11] K. J. Biba, Integrity Considerations for Secure Computer Sytems The MITRE Corporation, Tech. Rep., 1977.

[12] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in *Proc. NDSS*, San Diego, CA, 2001.

[13] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in *Proc. IEEE Symp. Security and Privacy*, Berkeley, CA, 2002.