A Secure & Scalable Access Method in Cloud Computing

Vandana Birle[1] Prof. Abhishek Raghuvanshi[2]

Abstract— Cloud computing has been envisioned as the next-generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective 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

To achieve flexible and fine-grained access control, a number of schemes have been proposed more recently. Unfortunately, these schemes are only applicable to systems in which data owners and the service providers are within the same trusted domain. Since data owners and service providers are usually not in the same trusted domain in cloud computing, a new access control scheme employing attributed-based encryption is proposed, which adopts the so-called key-policy attribute-based encryption (KP-ABE) to enforce fine-grained access control. However, this scheme falls short of flexibility in attribute management and lacks scalability in dealing with multiple-levels of attribute authorities.

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. 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 recipients ability to satisfy a policy in distributed systems. One of the encryption schemes is AttributeBased 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

All rights reserved by www.ijsrd.com

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.

III. PROPOSED SYSTEM

This proposed system 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.

We propose a novel encryption scheme for access control in cloud computing. The proposed work is an extension of ciphertext-policy attribute- set-based encryption (CP-ASBE, or ASBE for short) scheme .

A. *New Scheme:* In new scheme, a data encryptor specifies an access structure for a ciphertext which is referred to as the ciphertext policy. Only users with decryption keys whose associated attributes, specified in their key structures, satisfy the access structure can decrypt the ciphertext.

1) Basic Concepts Used

Key Structure: We use a recursive set based key structure as in [19] 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.

B. *Access Structure:* In our scheme, we use the same tree access structure as in [19]. 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 . An example of the access tree structure is shown in Fig., where the threshold values for " AND"and"OR"are2 and 1, respectively.

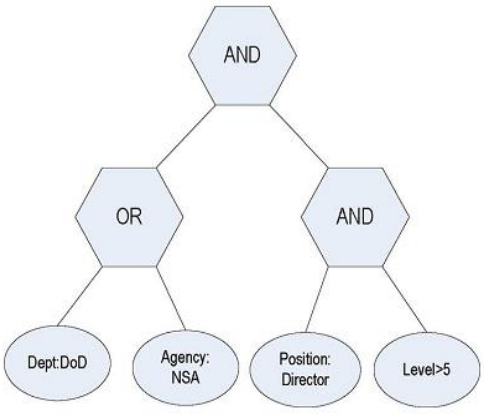

Figure. 1 : Access structure

– *The Scheme:*

We propose a novel encryption scheme for access control in cloud computing. The proposed work is an extension of ciphertext-policy attribute- set-based encryption (CP-ASBE, or ASBE for short) scheme.

Our scheme consists of a trusted authority, multiple domain authorities, and numerous users corresponding to data owners and data consumers. The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user's decryption key.

– *Our proposed scheme performs following operations:*

1) System Setup,
2) Top-Level Domain Authority Grant,
3) New Domain Authority/User Grant,
4) New File Creation,
5) User Revocation,
6) File Access,andFile Deletion.

IV. CONCLUSION

In this thesis, 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 by Bethencourt et al.. 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

All rights reserved by www.ijsrd.com

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.
[14] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2003.
[15] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. ACM Conf. Computer and Communications Security (CCS), Alexandria, VA, 2005.

[16] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[17] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542.

[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[19] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically
motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[20] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.

[21] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.
[22] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.
[23] D. Boneh and M. Franklin. Identity-Based Encryption from The Weil Pairing. In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.
[24] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In Proc. of CCS'06, New York, NY, USA, 2006.
[25] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data. In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.
[26] R. Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with
non-monotonic access structures". In Proc. of CCS'06, New York, NY, 2007.
[27] M. Chase. "Multi-authority attribute based encryption". In Proc. of TCC'07,
Amsterdam, Netherlands, 2007.
[28] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP'07, Washington, DC, USA, 2007.
[29] L. Cheung and C. Newport. Provably Secure Ciphertext Policy ABE. In Proc. of CCS'07, New York, NY, USA, 2007.
[30} B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization", http://eprint.iacr.org/2008/290.
[31] V. Goyal, A. Jain, O. Pandey and A. Sahai, "Bounded Ciphertext-Policy Attribute based Encryption", In Proc. of ICALP'08, Reykjavik, Iceland, 2008
[32] M. J. Hinek, S. Jiang, R. Safavi-Naini, and S. F. Shahandashti, "Attribute-Based Encryption with Key Cloning Protection", http://eprint.iacr.org/2008/478
[33] Jin Li, Qian Wang, Cong Wang, and Kui Ren, "Enhancing Attribute-based Encryption with Attribute Hierarchy," In Proc. of ChinaCom'09, Xi'an, China

All rights reserved by *www.ijsrd.com*