International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 5, May-2014, pp: (10-12), Impact Factor: 1.147, Available online at: www.erpublications.com

More Secure and Private Enhancement of Architectures in Cloud Environment: A Survey

Onkar D. Dike[1], Suhas H. Patil[2]
[1]M.Tech. [Computer], Bharati Vidyapeeth Deemed University, College of Engineering Pune, India
[2]Professor [Computer], Bharati Vidyapeeth Deemed University, College of Engineering Pune, India

Abstract: Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this system also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers. Access control is one of the most important security mechanisms in cloud computing. Attribute-based access control gives a flexible approach that allows data owners to integrate data access policies within the encrypted data. This addresses this challenging open issue by defining and enforcing access policies based on data attributes allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to entrusted cloud servers without disclosing the underlying data. We achieve this by exploiting and uniquely combining techniques of attribute-based encryption (ABE).

Keywords: SOA; KP-ABE; PRE; DBDH.

I. INTRODUCTION

Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. By combination of existing and new techniques from research areas such as Service-Oriented Architectures (SOA) and virtualization, cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet. Cloud computing provides an extensible and powerful environment for growing amounts of services and data by means of on-demand self-service. It also relieves the client's burden from management and maintenance by providing a comparably low-cost, scalable and location-independent platform. Along with this, various business models are developed, which can be described by terminology of Infrastructure as a services(IaaS), Platform as a services(PaaS) ,and Software as a services(SaaS). Successful examples are Amazon's EC2 and S3, Google App Engine, and Microsoft Azure which provide users with scalable resources in the pay-as-you use fashion at relatively low prices. Cloud computing is also facing many challenges that may impede its fast growth if they are not resolved.As compared to building their own infrastructures, users is able to save their investments significantly by migrating businesses in the cloud. With the increasing development of cloud computing technologies, that in the near future more and more businesses will be moved into the cloud. 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. The data owners want to keep information on cloud very confidential and they also want to take the maximum advantage of the resources that cloud provides. The data access control has been evolving in the past thirty years and various techniques have been developed to effectively implement fine grained access control. These techniques will allow flexibility in accessing data from different users in cloud environment. The available access control architectures usually assume the data owner and the servers which contains the same domain. Here the servers are fully entrusted responsible for defining and enforcing access control policies.

To access the data very smoothly the correct solution would be encrypting data through certain cryptographic policies and disclosing decryption keys only to authorized users. This general method actually has been widely adopted by existing works [3]-[5] which aims at securing data storage on entrusted servers. One challenging issue with this design is the implementation of user revocation, which would require re-encryption of data files accessible to the leaving user. It may need update of secret keys for all the remaining users. We achieve our design goals by exploiting key policy attribute-based encryption [6], and uniquely combine it with the technique of proxy re-encryption (PRE) [7] and lazy re-encryption [3].

II. TECHNIQUES USED

A. KeyPolicy Attribute-Based Encryption (KP-ABE)

KP-ABE [6] is a public key cryptography primitive for one-to-many communications. In KP-ABE, data is associated with attributes for each of which a public key component is defined. The set of attributes to the message by encrypting it with the corresponding public key components associated with the encryptor. A KP-ABE scheme is composed of four algorithms which can be defined as follows:

Setup: This algorithm takes as input a security parameter κ and the attribute universe U = {1, 2, . . .,N} of cardinality N. It defines a bilinear group G1 of prime order p with a generator g, a bilinear map e: G1 × G1 → G2 which has the properties of bilinearity, computability, and non-degeneracy. It returns the public key as well as a system master key MK as follows

PK = (Y, T1, T2, . . . , TN) MK = (y, t1, t2, . . . , tN)

where $T_i \in G1$ and $t_i \in Zp$ are for attribute i, $1 \leq i \leq N$, and $Y \in G2$ is another public key component. We have $T_i = g^{ti}$ and $Y = e(g, g)^y$, $y \in Zp$. While PK is publicly known to all the parties in the system, master key is kept as a secret by the authority party.

Encryption: This algorithm takes a message M, a set of attributes I as input and public key PK, It outputs the cipher text E with the following format: $E = (I, \tilde{} E, \{Ei\}\ i \in I)$ where $\tilde{}E = MY^s$, $Ei = T^s_i$, and s is randomly chosen from Zp.

Key Generation: This algorithm takes as input an access tree T, the master key MK, and the public key PK. It gives a user secret key SK as follows. It defines a random polynomial $p_i(x)$ for each node i of T in the top-down manner starting from the root node r. For each non-root node j,

$p_j(0) = p_{parent(j)}(idx(j))$

where parent(j) represents j's parent and idx(j) is j's unique index given by its parent.

For the root node r, $p_r(0) = y$. Then it outputs SK as follows.

$$SK = \{sk_i\}_{i \in L}$$

where L denotes the set of attributes attached to the leaf nodes of T and $sk_i = g^{pi\ /(0)\ ti}$.

Decryption: This algorithm takes as input the ciphertext E encrypted under the attribute set I which is the user's the public key PK and secret key SK for access tree T. First it computes $(E_i, sk_i) = e(g, g)^{pi(0)s}$ for leaf nodes. It aggregates these pairing results in the bottom-up manner using the polynomial interpolation technique. At the end it may recover the blind factor $Y^s = e(g, g)^{ys}$ and output the message M if and only if I satisfies T.

B. Proxy Re-Encryption (PRE)

Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under Alice's public key into another cipher text that can be opened by Bob's private key without seeing the underlying plaintext.

III. SECURITY ANALYSIS

The security analysis of the system is regarding of the following few factors

A. Fine Grained Access Control:

The data owner is able to define and enforce expressive and flexible access structure for each user. The access structure of each user is defined as a logic formula over data file attributes, which is able to represent any desired data file set.

B. User Secrete Key Accountability:

This property can be immediately achieved by using the enhanced construction of KP-ABE which can be used to disclose the identities of key abusers. We analyze data confidentiality of the system by giving a cryptographic security proof.

C. Data Confidentiality:

We analyze data confidentiality of the system by comparing it with an intuitive scheme in which data files are encrypted using symmetric DEKs. These DEKs are encrypted directly using standard KP-ABE. In the system just cipher text of files are given to the cloud servers. The standard KP-ABE is provably secured under the attribute-based Selective-Set model [6] given the Decisional Bilinear Diffie-Hellman (DBDH) problem is hard.

IV. SUMMARY

Although ABE provides secure and fine-grained access control, before its deployment in cloud computing, two critical security aspects have to be addressed, which are, 1) efficient user revocation; 2) user accountability. In access control systems, when a user's access privilege is to be revoked, traditional revocation techniques, such as [10], can be used. However, for scalability purpose, it is necessary to enable efficient revocation operation. With the ABE technique to realize the fine-grained access control, the user accountability is implemented by using the traitor tracing technique. Clearly, to securely deploy an ABE-based access control system, it is imperative to guarantee that the key issued to each user cannot be shared. Such key abuse problem exists in ABE-based access control schemes [11] as their attribute keys are never designed to be linked to any user specific information except the commonly shared attributes.

REFERENCES

[1]. H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. of NDSS'01, 2001.
[2]. W. H. Winsborough and J. Li, N. Li, , "Automated trust negotiation using cryptographic credentials," in Proc. of CCS'05, 2005.
[3]. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable secure file sharing on untrusted storage," in Proc. of FAST'03,
[4]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," inProc. of NDSS'05, 2005.
[5]. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proc. of VLDB'07, 2007.
[6]. Shucheng Yu, Cong Wang, Kui Ren , and Wenjing Lou. " Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", in IEEE INFOCOM ,2010.
[7]. M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. of EUROCRYPT '98, 1998.
[8]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," inProc. of ESORICS '09, 2009.
[9]. L. Youseff, M. Butrico, and D. D. Silva, "Toward a unified ontology of cloud computing," in Proc. of GCE'08, 2008.
[10]. BennyChor, Amos Fiat, and MoniNaor. Tracing Traitor. CRYPTO'94, LNCS 839, pp. 257-270, Springer, 1994.
[11]. Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, IEEE INFOCOM, 2010.