International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 9, September-2018

IMPLEMENTATION OF ROBUST CONTROL OF PRSONALIZED BASED ON IMPROVING SECURITY LOCATION AWARE IN CLOUD STORAGE

V.S.Susmitha Arosan [#1], Mr.S Muruganandam [#2],

M.Phil (full-time) Research Scholar, Assisstant Professor,
PG and Research Department of Computer Science,
Vivekananda College of Arts and Sciences for Women,
Elayampalayam, Tiruchengode, Namakkal, Tamilnadu, India.

Abstract

In cloud computing data access control is a challenging in public cloud storage system This is a vendor neutral conceptual model that Ciphertext-Policy Attribute-Based Encryption (CP-ABE) concentrates on the role and interactions of the identified actors in the cloud computing sphere, that flexible for securable data and access control for cloud storage with honest-but-curious cloud servers. An CA (Central Authority) is introduced to generate secret keys for legitimacy verified users. Unlike other multiple authority access control schemes, each authority in their own scheme manages the whole attribute set individually. The framework employs multiple attribute authorities to share the load of user legitimacy verification. To address the issue of data that access control in cloud storage, there have been quite a few schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques.

Index Term- Cloud Storage, Access Control, Auditing, CPABE.

1. Introduction

Cloud storage is a promising and important service paradigm in cloud computing. Benefits of using cloud storage includes great accessibility, higher and rapid deployment for stronger protection. Ciphertext Policy Attribute based Encryption (CP-ABE), similarly with role-based access control system, that can widely Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fees provided for that's copies are not made or distributed for profit. These standards will be driven by operational requirements of the agencies and through collaboration with Agency CIOs, private sector experts, and international bodies to identify, prioritize, and reach consensus on standardization priorities. By keeping this focused to a role based structure, we alleviate the need for developing a technically-based architecture at this time Professor" or ("Computer Science" and "Teaching Assistant"). The server is entrusted as a reference monitor that checks the users legal certification before allowing him to access records or files. Portability and Interoperability that supports the migration of services and data between clouds. Cloud carriers provide access to consumers through network, but these are unable to efficiently handle more expressive types of encrypted access controls that could be a set of attributes that are linked with logical operators, such as AND and OR. Every single data file is associated with a set of attributes.

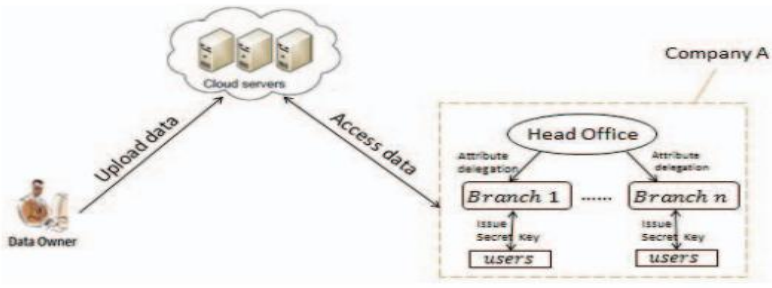

Figure 1. Our application scenario

Based on the analysis, summaries are the contributions as follows:

1.1We propose decentralized CP-ABE scheme (CP-DABE)

1. The scheme makes the process of issuing secret keys for users not to be centralized by the head office. The scheme provides a secure attribute delegation services between the head office and its distributed branches. In other words, the scheme lets the head office delegate a set of attributes to each of its branches. Each branch in turn uses these attributes to issue secret keys for its users.

2. Each affected branch in turn uses this proxy key to update the corresponding attribute keys assigned to its users secret keys. The second proxy key will be delegated to the cloud provider, which in turn uses this proxy key to update the corresponding attribute keys assigned to any data without disclosing the underlying data content. The data owners will not get involved in the revocation process since the cloud provide will update attribute keys assigned to any data in a secure manner.

3. The CP-DABE reduces the computational We achieved this by building the CP-DABE construction upon the efficient CP-ABE construction proposed by Waters requirements compared with the most relevant work. . In CPDABE, we extended the Waters scheme by supporting the attribute delegation and revocation, while keeping the computational cost for all CP-DABE algorithms as low as possible. The Waters scheme provides the basic CP-ABE algorithms (i.e. setup, keygen, encrypts, and decrypt algorithm), and is not designed for a large-scale environment.

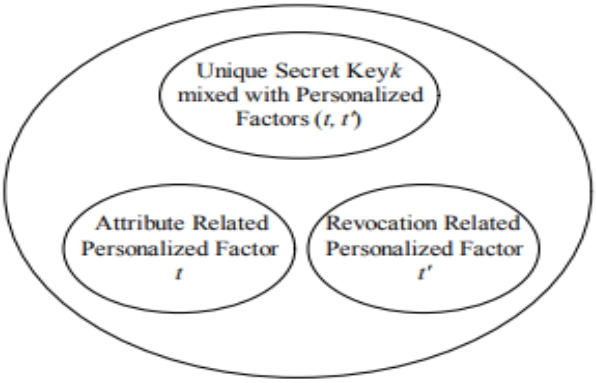

Figure 2. The components of secret key

4. The most important usage of concept hierarchy is to distinguish meanings for classification or exploit semantic similarities.

2. Literature survey

The cryptographic assumptions as expressive as. To improve efficiency of this encryption technique, Emura et al. This schemes which are only limited to express monotonic access structures, obtrovsky etal. proposed a more expressive CP-ABE scheme which can support non-monotonic access structures. ABE technique for CPABE which enables the user to do as much pre-computation as possible to save online computation.

2.1 Linear Secret Sharing Schemes

` 1.There exists a matrix M called the share-generating matrix for π. The matrix M has l rows and n columns. For all i = 1, · · · , l, the i'th row of M we let the function ρ defined the party labeling row i as ρ(i). When we consider the column vector v = (s, r2, · · · , rn), where s ∈ Zp is the secret to be shared, and r2, · · · *, rn ∈ Zp are randomly chosen, then Mv is the vector of l shares of the secret s according to π. The share (Mv)i belongs to party ρ(i).

S ∈ A 2 be any authorized set, and let I ⊂ {1, 2, · · · , l} be defined as I = {i : ρ(i) ∈ S}. If {λi} are valid shares of any secret s according to π, then ∑ i∈I ωiλi = s. Also, these constants ωi can be found in time polynomial in the size of the share generating matrix M.

2.2 Background

The value of one attribute concept can be numerical or categorical. Next, we give background information on bilinear maps. Like the work of Goyal et al. we define an access structure and use it in our security definitions. A categorical value can be mapped to the number of times that the value occurred in the dataset when such a hierarchy is unavailable

2.3 System Model

Corresponding to the scenario given in multiple domain masters (DMs) in which the top-level DMs correspond to the branches, and numerous users that correspond to users in the scenario. RM is responsible for generating the public parameters and delegating a set of attributes to DMs in the next level. DM is responsible for delegating a subset of its attributes to DMs in the next level that correspond to the department of the branch. Each DM administers a number of users in the next level. The users obtain their secret keys from their administering DM. The users use their secret keys to access data files stored in cloud providers' domains. For the sake of simplicity, in the CP-DABE, we assume that there is only one cloud provider.

3. Related Work

In this paper, we present an efficient heterogeneous framework with single CA/multiple AAs to address the problem of single-point performance bottleneck. The novel idea of our proposed scheme is that the complicated and time-consuming user legitimacy verification is executed only once by one selected AA. Furthermore, an auditing mechanism is proposed to ensure the traceability of malicious AAs. Thus our scheme can not only remove the single-point performance bottleneck but also be able to provide a robust, high-efficient, and secure access control for public cloud storage. This scheme actually addressed the single-point bottleneck on both security and performance in CP-ABE based access control in public cloud storage.

3.1 Preliminaries And Definitions

A. Bilinear Maps Let G, GT be two multiplicative cyclic groups with the same prime order p, and g be a generator of G. A bilinear map e : G × G → GT defined on G has the following three properties: 1) Bilinearity: ∀a, b ∈ Zp and g1, g2 ∈ G, we have e(g a 1 , gb 2) = e(g1, g2) ab . 2) Non-degeneracy: ∀g1, g2 ∈ G such that e (g1, g2)≠ 1, which means the map does not send all pairs in G × G to the identity in GT . 3) Computability: There is an efficient algorithm to compute e(g1, g2) for all g1, g2 ∈ G

Definition 1.

Decisional q-parallel Bilinear Diffie-Hellman Exponent Assumption(decisional q-BDHE): The decisional qBDHE problem is that, in a group G of prime order p, give a, s, b1, b2, . . . , bq ∈ Zp, if an adversary is given: $\vec{y}$ = (g, gs , ga , . . . , g(a q) , g(a q+2) , . . . , g(a 2q) ∀1≤j≤q,gs·bj , ga/bj , . . . , g(a q/bj) , g(a q+2/bj) , . . . , g(a 2q/bj) ∀1≤j,l≤q,l≠j , ga·s·bl/bj , . . . , ga q ·s·bl/bj), it must remain hard to distinguish e(g, g) a q+1s ∈ GT from a random element R in GT .

Definition 2

Linear Secret Sharing Schemes (LSSS): A secretsharing scheme Π over a set of parties P is called linear (over Zp) if: 1) The shares for each party form a vector over Zp. 2) There exists a matrix an M with l rows and n columns, which is called the sharing-generating matrix for Π. For all i = 1, ..., l, the i-th row of M is labeled by a party ρ(i), where ρ is the function associating rows of M to parties in P. When we consider the vector $\vec{v}$ = (s, r2, ..., rn) ∈ Z n p , where r2, ..., rn are randomly chosen and s is the secret to be shared, then $\vec{\lambda}$ = M×$\vec{v}$T is the vector of l shares of the secret s according to Π. The share λi belongs to the party ρ(i).

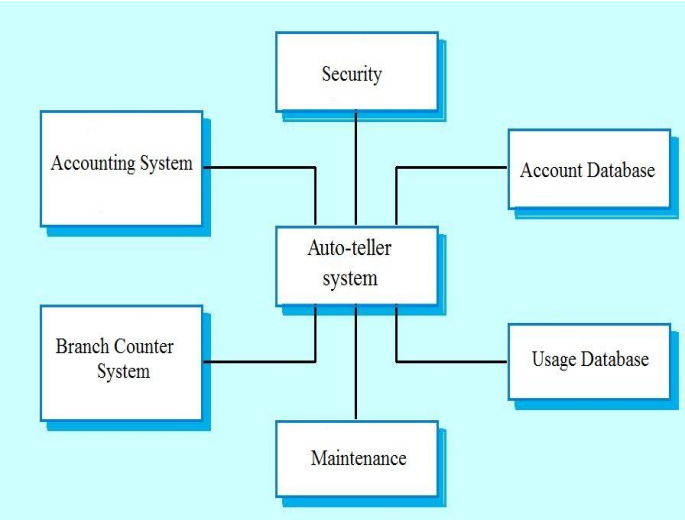

Figure 3: System Model

3.2 The data owner (Owner)

The access policy about who can get access to each file, and encrypts the file under the defined policy. After that, the owner sends the whole encrypted data and the encrypted symmetric key (denoted as ciphertext CT) to the cloud server to be stored in the cloud.

3.3.1Data confidentiality

Data content must be kept confidential to unauthorized users as well as the curious cloud server.

1. Collusion-resistance. Malicious users colluding with each other would not be able to combine their attributes to decrypt a ciphertext which each of them cannot decrypt alone.

2. AA accountability. An auditing mechanism must be devised to ensure that an AA's misbehavior can be detected to prevent AAs' abusing their power without being detected.

3. No ultra vires for any AA. An AA should not have unauthorized power to directly generate secret keys for users. This security equirement is newly introduced based on our proposed hierarchical framework.

3.3.2 Analysis and Result

AAs are stand by for the legitimacy verification in the system. There is a key request, an idle AA is selected by a scheduling algorithm to perform the verification and others.

3.3 Modeling in Queuing Theory

It's important to note that some other strategies can also be adopted in our architecture, such as a user arriving at a nearest AA according to his/her knowledge and decisions.

The following assumptions are made to describe our system.

1) Assumption 1. The instant user request arrival event constitutes a stationary Poisson process with the parameter λ.

2) Assumption 2. For each AA, the service time of different individual users are independent and identically distributed exponential random variables, in which the mean value is $1/\mu 1$.

3) Assumption 3. For CA, the service time of individual users are independent and identically distributed exponential random variables, in which the mean value is $1/\mu 2$.

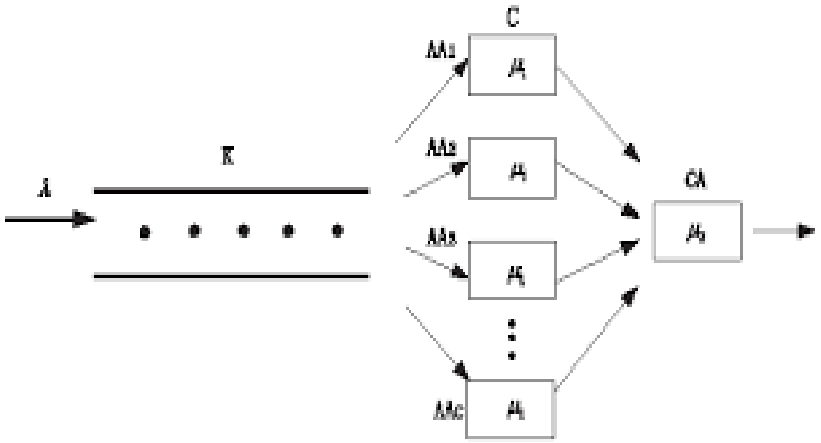

Figure 4: The queue model with single- CA/multi-AAs

4. Conclusion

The security analysis shows that our scheme could effectively resist to individual and colluded malicious users, as well as the honest-but-curious cloud servers. Besides, with the proposed auditing & tracing scheme, no AA could deny its misbehaved key distribution. Our proposed scheme provides a fine-grained, robust and efficient access control with one-CA/multi-AAs for public cloud storage.

Feature of Acceleration mode compared to software simulator	Hardware emulation	Signal-based acceleration	Transaction based acceleration	
Speedup1x	1,500x	<100x	<1,500x	<1,500x
Test bench Compatitabilitu	Poot	Excelent	Poor	Fari
Communication Overhead	No	Very High	Low	No
Hardware Over head	No	No	Low	Low

Table 1: Communication Overview

5. Reference:

[1] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS 2007). ACM, 2007, pp. 195–203.

[2] S. Hohenberger and B. Waters, "Online/offline attributebased encryption," in Public-Key Cryptography–PKC 2014. Springer, 2014, pp. 293–310.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2010). ACM, 2010, pp. 261–270.

[4] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts." in USENIX Security Symposium, vol. 2011, no. 3, 2011.

[5] J. Shao, R. Lu, and X. Lin, "Fine-grained data sharing in cloud computing for mobile devices," in Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM 2015). IEEE, 2015, pp. 2677–2685.

[6] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, 2014.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005. Springer, 2005, pp. 457–473.

[8] M. Chase, "Multi-authority attribute based encryption," in Proceedings of the 4th Theory of Cryptography Co.