SECURE KEY POLICY ATTRIBUTE BASED ENCRYPTION AND DECRYPTION

A.GOPALA KRISHNAN[1],K.KRISHNA RAJ[2],G.ARAVINTHA NARAYANA SUBBU[3],A.RAJARAJESHWARAN[4]

1.Assistant Professor,Dept Of CSE,Gnanamani college of Technology,Namakkal-637018.
2.Final Year UG Student, ,Dept Of CSE,Gnanamani college of Technology,Namakkal-637018.
3. Final Year UG Student, ,Dept Of CSE,Gnanamani college of Technology,Namakkal-637018.
4. Final Year UG Student, ,Dept Of CSE,Gnanamani college of Technology,Namakkal-637018.

ABSTRACT- As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of re-encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE). In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast re-encryption with TPA. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Re-Encryption (HIBR).

INTRODUCTION

The network and computing technology enables many people to easily share their data with others were using online external storages. People can share their lives with friends by uploading their private photos or messages into the online for ease of sharing with their primary doctors or for cost saving.As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise.Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data.People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. Attribute-based encryption (abe) is a promising cryptographic approach that achieves a fine-grained data access control it provides a way of defining access policies based on different attributes of the requester, environment, or the data object.

Especially, cipher text policy attribute-based encryption (KP-ABE) enables an Encrypt or to define the attribute set over a universe of attributes that a decryption needs to possess in order to decrypt the cipher text, and enforce it on the contents.This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access, which is the traditional access control approach of such as the reference monitor.Nevertheless, applying KP-ABE in the data sharing system has several challenges.In KP-ABE, the key generation center (KGC) generates private keys of users by applying the KGC's master

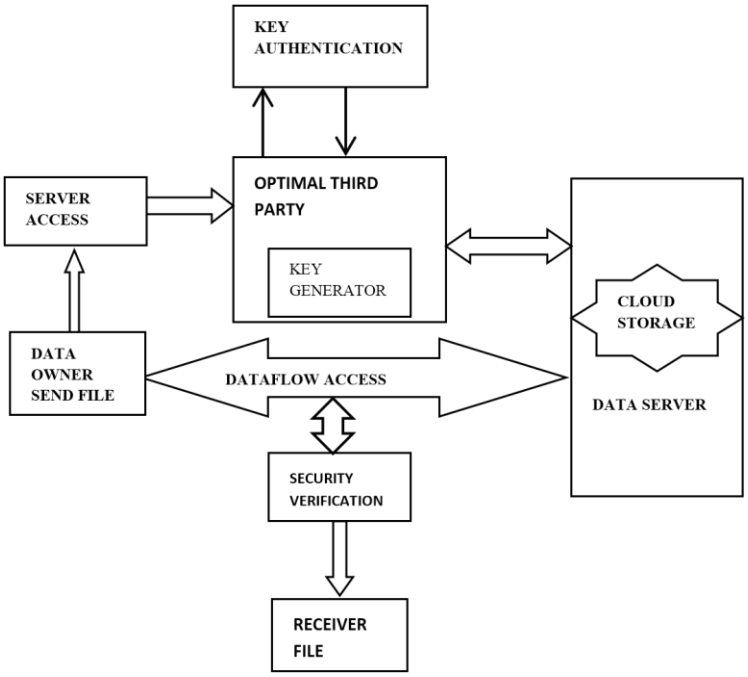
secret keys to users' associated set of attributes.Thus, the major benefit of this approach is to largely reduce the need for processing and storing public key certificates under traditional public key infrastructure (PKI).

RELATED WORK

We develop a variation of the KP-ABE algorithm partially based on (but not limited to) construction in order to enhance the expressiveness of the access control policy instead of building a new KP-ABE scheme from scratch. Its key generation procedure is modified for our purpose of removing escrow. The proposed scheme is then built on this new KP-ABE variation by further integrating it into the proxy encryption protocol for the user revocation.

To handle the fine-grained user revocation, the data storing center must obtain the user access (or revocation) list for each attribute group which is related to TPA permission generated code, since otherwise revocation cannot take effect after all.This setting where the data-storing center knows the revocation list does not violate the security requirements, because it is only allowed to re encrypt the cipher texts .This authentication and can by no means obtain any information about the attribute keys of users only accessed by valid users.

Cao et al.proposed the multikeyword ranked search over encrypted data for the first time and built a searchable index based on the vector space model, and chosen "coordinate matching" to measure the similarity between queries and documents. However, in their schemes, the time complexity of search is $O(nm)$ (n is the number of keywords in dictionary, m is the size of the documents that stored in the cloud server), and the time complexity of trapdoor construction is also very high. Sun et al. proposed a tree-based index structure which is based on the vector space model and the TF× IDF model. This structure achieves sub-linear time complexity, but it is vulnerable in protecting data privacy. One step further, Xia et al. proposed a Greedy Depthfirst Search treebased searchable encryption scheme EDMRS, which achieved more efficiency than early works, but the cost of search remains high and the time complexity of creating trapdoor is high.



The system model of searching over outsourced encrypted data and Decrypted data

Therefore, the proposed scheme achieves more secure and fine-grained data access control in the data sharing system.We demonstrated that the proposed scheme is efficient and scalable to securely manage user data in the data sharing system.

Finegrained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified.

PROBLEM FORMULATION

In several distributed systems a user should only be able to access data if a user possess a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Cipher textPolicy Attribute-Based Encryption.

Our techniques. At a high level, our work is similar to the recent work of Sahai and Waters and Goyal et al. on key-policy attribute based encryption (KP-ABE), however we require substantially new techniques. In keypolicy attribute based encryption, ciphertexts are associated with sets of descriptive attributes, and users' keys are associated with policies (the reverse of our situation). *We stress that in keypolicy ABE, the encryptor exerts no control over who has access to the data she encrypts, except by her choice of descriptive attributes for the data.* Rather, she must trust that the keyissuer issues the appropriate keys to grant or deny access to the appropriate users. In other words, in, the "intelligence" is assumed to be with the key issuer, and not the encryptor. In our setting, the encryptor must be able to intelligently decide who should or should not have access to the data that she encrypts. As such, the techniques of do not apply to our setting, and we must develop new techniques.

At a technical level, the main objective that we must attain is *collusion-resistance*: If multiple users collude, they should only be able to decrypt a ciphertext if at least one of the users could decrypt it on their own. In particular, referring back to the example from the beginning of this Introduction, suppose that an FBI agent that works in the terrorism office in San Francisco colludes with a friend who works in the public corruption office in New York. We do not want these colluders to be able to decrypt the secret memo by combining their attributes. This type of security is the *sine qua non* of access control in our setting.

We created a system for CiphertextPolicy Attribute Based Encryption. Our system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. Our system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. Finally, we provided an implementation of our system, which included several optimization techniques.

The proposed scheme can do an immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the cipher text policy attribute-based encryption. Therefore, the proposed scheme achieves more secure and finegrained data access control in the data sharing system. We demonstrated that the

proposed scheme is efficient and scalable to securely manage user data in the data sharing system.

MODULE DESCRIPTION

1.Cryptographic key assumption:

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. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphism token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s).

Attribute key assumption:

Group key distribution schemes has recently received a lot of attention from the researchers, as a method enabling large and dynamic groups of users to establish group keys over unreliable network for secure multicast communication. In such schemes, time is divided into epochs called sessions. At the beginning of each session, a Group Manager transmits some broadcast message, in order to provide a common key to each member of the group. Every user, belonging to the group, computes the group key using the message and some private information.

The main property of the scheme is that, if some broadcast message gets lost, then users are still capable of recovering the group key for that session by using the message they received at the beginning of a previous session and the message they will receive at the beginning of a subsequent one, without requesting additional transmission from the Group Manager.

This approach decreases the workload on the Group Manager and reduces network traffic as well as the risk of user exposure through traffic analysis.

Key distribution:

Common group key is frequently updated to ensure secure multicast communication. Group lifetime is dived into epochs called sessions; single key instance is valid only throughout one session. Group membership can change between consecutive sessions.

Moreover, to effectively remove a node from multicast group, who is willing to leave, or is forced to leave, a new session must begin and nodes from shall start protecting group communication using a new, which is not accessible to Thus, the choice of session length is a tradeoff between key distribution cost in terms of communication and computational overhead, and the required security level.

Key issuing secured access:

To handle the fine-grained user revocation, the data storing center must obtain the user access (or revocation) list for each attribute group, since otherwise revocation cannot take effect after all.

This setting where the data-storing center knows the revocation list does not violate the security Requirements, because it is only allowed to re encrypt the cipher texts and can by no means obtain any information about the attribute keys of users. Since the proposed scheme is built on, we recapitulate some definitions in to describe our construction in this section, such as access

tree, encrypt, and decrypt algorithm definitions.

Security analysis

Security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely digital signature, message authentication code, and encryption, in our system. The fraud can be repudiated only if the client can provide a different representation he knows of from the trusted authority (TA).

Fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified.

PERFORMANCE MEASUREMENTS

We now provide some information on the performance achieved by the Kpabe toolkit. The measurements of private key generation time, encryption time, and decryption time produced by running Kpabekeygen, Kpabe-enc, and Kpabe-dec on a range of problem sizes. The measurements were taken on a modern workstation. [1] The implementation uses a 160-bit elliptic curve group based on the supersingular curve $y^2 = x^3+x$ over a 512-bit finite field. On the test machine, the PBC library can compute pairings in approximately 5.5ms, and exponentiations in G_0 and G_1 take about 6.4ms and 0.6ms respectively. Randomly selecting elements (by reading from the Linux kernel's /dev/urandom) is also a significant operation, requiring about 16ms for G_0 and 1.6ms for G_1.

As expected, Kpabe-keygen runs in time precisely linear in the number of attributes associated with the key it is issuing. The running time of Kpabe-enc is also almost perfectly linear with respect to the number of leaf nodes in the access policy. The polynomial operations at internal nodes amount to a modest number of multiplications and do not significantly contribute to the running time. Both remain quite feasible for even the largest problem instances.

CONCULSIONS

The proposed an attribute based data sharing scheme to enforce a fine-grained data access control by exploiting the characteristic of the data sharing system. The user secret keys are generated through a secure two-party computation such that any curious key generation center or data-storing center cannot derive the private keys individually.

The data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials. The scheme can do an immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the cipher text policy attributebased encryption. Achieves more secure and fine-grained data access control in the data sharing system. We demonstrated that the proposed scheme is efficient and scalable to securely manage user data in the data sharing system

REFERENCES

[1] A. Sahai And B. Waters, "Fuzzy IdentityBased Encryption," In Advances In Cryptology (Lecture Notes In Computer Science), Vol. 3494,R. Cramer, Ed. Berlin, Germany: SpringerVerlag, 2014, Pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, And B. Waters, "Attribute-Based Encryption For fine-Grained Access Control Of Encrypted Data," In Proc.Acmconf. Comput. Commun. Secur., 2006, Pp. 89-98.

[3] J. Bethencourt, A. Sahai, And B. Waters, "Ciphertext-Policy Attributebased Encryption," In Proc. Ieee Symp. Secur. Privacy, May 2016,Pp. 321–334.

[4] B. Waters, "Ciphertext-Policy AttributeBased Encryption: An Expressive, Efficient, And Provably Secure Realization," In Public Key Cryptography (Lecture Notes In Computer Science), Vol. 6571, D. Catalano, N. Fazio, R. Gennaro, And A. Nicolosi, Eds. Berlin, Germany: Springer-Verlag,2011, Pp. 53–70.

[5] Alliance ,"Top Threats To Cloud Computing, "Practical Constructions And New Proof Methods For Large Universe Attribute-Based Encryption," In Proc. Acmconf. Comput. Commun. Secur., 2013, Pp. 463–474.

[6] L. Cheung And C. Newport, "Provably Secure Ciphertext Policy Abe,"In Proc. Acm Conf. Comput. Commun. Secur., 2013, Pp. 456–465.

[7] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. De Panafieu, And C. Ràfols, "Attribute-Based Encryption Schemes With ConstantSizeciphertexts," Theoretical Comput. Sci., Vol. 422, Pp. 15–38, Mar. 2012.

[8] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao And B. Waters, "Possible Decrease Of Spam In The Email Communication," In Proc. 20th Usenix Secur. Symp., 2016, P. 34.

[9] J. Lai, R. H. Deng, C. Guan, And J. Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption," Ieee Trans. Inf. Forensicssecurity, Vol. 8, No. 8, Pp. 1343–1354, Aug. 2013.

[10] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue," Towards Secure Multi-Keyword Top-K Retrieval Overencrypted Cloud Data]," In Advancesin Cryptology (Lecture Notes In Computer Science), Vol. 6223, T. Rabin, Ed. Berlin, Germany: SpringerVerlag, 2016, Pp. 465–482.