JES
Journal of Engineering Sciences

Vol 13, Issue 03, MARCH /2022

ISSN NO:0377-9254

EFFICIENT DECENTRALISED ATTRIBUTE BASED ACCESS CONTROL FOR MOBILE CLOUDS

[1]THALLAPALLY HARSITHA, [2]D SAIKRISHNA
[1]MCA Student, [2]Assistant Professor
Department Of MCA
Sree Chaitanya College Of Engineering, Karimnagar

ABSTRACT

Fine grained access control is a requirement for data stored in untrusted servers like clouds. Owing to the large volume of data, decentralized key management schemes are preferred over centralized ones. Often encryption and decryption are quite expensive and not practical when users access data from resource constrained devices. We propose a decentralized attribute based encryption (ABE) scheme with fast encryption, outsourced decryption and user revocation. Our scheme is very specific to the context of mobile cloud as the storage of encrypted data and the partial decryption of ciphertexts are dependent on the cloud and users with mobile devices can upload data to the cloud or access data from it by incurring very little cost for encryption and decryption respectively. The main idea is to divide the encryption into two phases, offline preprocessing phase which is done when the device is otherwise no in use and an online phase when the data is actually encrypted with the policy. This makes encryption faster and more efficient than existing decentralized ABE schemes. For decryption outsourcing, data users need to generate a transformed version of the decryption key allowing an untrusted proxy server to partially decrypt the ciphertext without gaining any information about the plaintext. Data users can then fully decrypt the partially decrypted ciphertext without performing any costly pairing operations. We also introduce user revocation in this scheme without incurring too much additional cost in the online phase. Comparison with other ABE schemes shows that our scheme significantly reduces computation times for both data owners and data users and highly suitable for use in mobile devices.

1. INTRODUCTION

Consider the common scenario where data owners want to upload their data for long-term storage to untrusted servers such as the cloud. The data may initially reside in resource constrained devices such as mobile phones, wireless sensors or smartcards. The aim is to store the data over a long time and allow multiple users to access the data. Cloud Service Providers (CSPs) today provide such seemingly unlimited storage facilities and are thus rapidly gaining popularity among individual data owners as well as enterprises with limited budgets. In spite of the benefits provided by CSPs, they are assumed to be malicious and data owners generally do not trust them with their sensitive data. So, any data stored in the cloud must be encrypted.

Moreover, data owners may wish to impose access control measures on data so that only users who have certain credentials can access it. For example, a hospital may wish to upload to the cloud the results of a clinical trial recording the response of cancer patients to a new drug. This data is sensitive and the hospital may want only the doctor attending a patient or a researcher involved in the drug discovery to have access to the data. Encryption schemes such as attribute-based encryption (ABE) [13], [39] provide great flexibility in terms of access control on encrypted data and are ideal for this scenario

In practice, decentralized or multi-authority ABE schemes are very useful as they do not need any central authority for generation and distribution of decryption keys related to different attributes. For example, the doctor who wants to access a patient's health record for diagnosis may be provided the relevant key by the hospital but a medical researcher may be given access to the same data by a medical research organization. User attributes are subject to periodic changes due to change in the work environment, location etc. [22]. Thus, a user who was previously granted access to data may no longer qualify for the access. Unless previously allotted keys are updated and the user is revoked, the user may continue to access the data in spite of a change in his attributes. So, user revocation is a necessary and useful property for ABE schemes. The use of these sophisticated encryption schemes pose one severe problem.

The encryption, revocation key generation and decryption phases are usually very costly, involving several bilinear pairing operations, and resource constrained devices are not suitable for performing such operations fast enough. To address this problem, we propose a decentralized attribute based encryption (ABE) scheme with fast encryption, outsourced decryption and user revocation. Our scheme is very specific to the context of mobile cloud as the storage of encrypted data and the partial decryption of Drop box are dependent on the cloud and users with mobile devices can upload data to the cloud or access data from it by incurring very little cost for encryption and decryption respectively.

As a solution to the costly encryption problem, we divide the encryption phase into an offline phase and an online phase, such that, most of the costly operations are performed offline when the user does not immediately expect the encryption to be completed, the device is charging or otherwise not in use. The online phase has little computations so that users can get on with their work without the device's performance being affected in any respect.

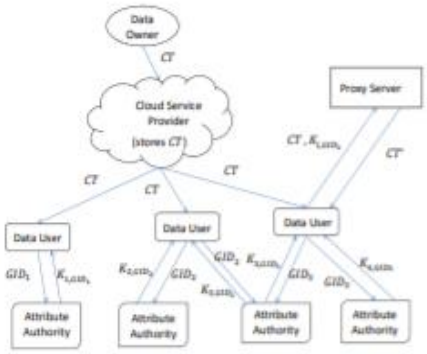
Data users are relieved from performing costly decryption operations by outsourcing such operations to a proxy server. The proxy server, using a transformed decryption key, partially decrypts the cipher text. However, the partial decryption process does not reveal any information to the malicious proxy server. Then, the data user needs to perform only a few simple operations to derive the final plaintext from the partially decrypted cipher text. Similarly, revocation keys can be generated offline, with a few computations in the online phase for key transformation before they are given to the proxy server.

We describe two motivating scenarios for our scheme. 1) Wireless sensor networks are widely used in healthcare to provide assistance to aging patients at home by collecting data about the physical, physiological and behavioral states and patterns from their living spaces. These sensitive personal data must be encrypted before long-term storage. Caregivers access this data for early detection and intervention, whereas researchers may access this data for studying the environmental contexts, illnesses and aging While caregivers can obtain the relevant attributes to access the data from a hospital, researchers may have to obtain them from universities and research organizations. 2) Employees from different organizations may be involved in collaborative projects where team members access certain data and make some contributions.

While on the move, a team member may upload his contribution to data storage services like Drop box from his mobile device. The data must be encrypted before

uploading as it may be sensitive (financial data, trade secrets etc.). Another person can access this data if he is a member of the project. However, the attribute indicating project membership may be assigned to each member by the organization it belongs to.

2. SYSTEM ANALYSIS



SYSTEM ARCHITECTURE

EXISTING SYSTEM

Decentralized or multi-authority ABE schemes are very useful as they do not need any central authority for generation and distribution of decryption keys related to different attributes. For example, the doctor who wants to access a patient's health record for diagnosis may be provided the relevant key by the hospital but a medical researcher may be given access to the same data by a medical research organization.

Owing to the large volume of data, decentralized key management schemes are preferred over centralized ones. Often encryption and decryption are quite expensive and not practical when users access data from resource constrained devices.

PROPOSED SYSTEM

Our scheme is very specific to the context of mobile cloud as the storage of encrypted data and the partial decryption of ciphertexts are dependent on the cloud and users with mobile devices can upload data to the cloud or access data from it by incurring very little cost for encryption and decryption respectively. The main idea is to divide the encryption into two phases, offline preprocessing phase which is done when the device is otherwise not in use and an online phase when the data is actually encrypted with the policy. This makes encryption faster and more efficient than existing decentralized ABE schemes. For decryption outsourcing, data users need to generate a transformed version of the decryption key allowing an untrusted proxy server to partially decrypt the ciphertext without gaining any information about the plaintext. Data users can then fully decrypt the partially decrypted ciphertext without performing any costly pairing operations. We also introduce user revocation in this scheme without incurring too much additional cost in the online phase. Comparison with other ABE schemes shows that our scheme significantly reduces computation times for both data owners and data users and highly suitable for use in mobile devices

3. IMPLEMENTATION

- **Data Owner Module**

In this module, the data owner uploads their data in the public cloud server. For the security

purpose the data owner encrypts the data file and assigns the digital sign and then store in the cloud. The data owner can check the data integrity of the file over Corresponding cloud server. The Data owner can have capable of manipulating the encrypted data file and data owner can update the file contents as well as delete his own file.

- **AA**

In this module, the AA Generates the Secret Key requested by the data user, the AA checks the file if present generates the appropriate Secret Key. The KG-CSP allows viewing the Secret Key generated files and also the transactions related to the file.

- **Proxy Server**

The server will manage and authorize PKC and maintain all data transactions between data owner and cloud server, end user.

- **Data User Module**

In this module, Data user logs in by using his user name and password. After he will request for secret key of required file from **CSP**, and get the secrete key from KGC. After getting secrete key he is trying to download file by entering file name and secrete key from cloud server.

- **Data Encryption and Decryption**

All the legal users in the system can freely query any interested encrypted and decrypted data. Upon receiving the data from the server, the user runs the decryption algorithm Decrypt to decrypt the cipher text by using its secret keys from different Users. Only the attributes the user possesses satisfy the access structure defined in the cipher text CT, the user can get the content.

- **Attacker Module**

In Data user module, while downloading time if remote user enters wrong trapdoor or secrete key then he is treated as Digital sign attacker or Secret Key attacker.

- **Data Integrity Check**

Data will be verified in the cloud to check it is integrated by attacker or not. If it is integrated then it is recovering from the data owner.

4. CONCLUSIONS

In this paper we build a CPABE scheme in prime order. As pointed out by [29], the proof of the scheme is in the generic group model using random oracles. The reason for using prime order groups is that the schemes are efficient with faster group operations. Our construction can be used to design a scheme in composite order group, which though inefficient, rests on stronger notions of security in the dual system encryption model [42]. We leave it as a future work. This paper can address the following problems (with or without revocation): 1) Online-offline multi-authority CPABE with decryption outsourcing (Section IV) and 2) Online offline multi-authority CPABE (Appendix VIII). One problem with decryption outsourcing is that the user does not know if the partial decryption was correct. To overcome this, verifiable outsourcing was proposed in [25]. A similar technique can be used to address verifiable outsourcing in our problem. We do not address it here as ours is an honest-but-curious model. Relaxing this assumption makes it important to study verifiable decryption outsourcing. We leave it as an open problem. In this paper, we propose an ABE scheme suitable for mobile clouds. It combines the useful properties of decentralization, fast encryption, outsourced decryption and user revocation. All heavy computations related to encryption are performed during the offline phase making the whole encryption phase faster and more efficient than existing decentralized ABE schemes. An untrusted proxy server partially decrypts the cipher text without gaining any information about the plaintext. Data users can then fully decrypt the partially decrypted cipher text without performing any costly pairing operations. Our scheme supports user revocation without

incurring much additional cost in the online phase. Overall, unlike other existing works, our scheme hits a good balance between encryption and decryption performance, while supporting additional useful properties such as decentralization and user revocation.

REFERENCES

[1] N. Attrapadung and H. Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.

[2] N. Attrapadung and H. Imai. Conjunctive broadcast and attribute-based encryption. In Pairing-Based Cryptography-Pairing 2009: Third International Conference Palo Alto, CA, USA, August 12-14, 2009 Proceedings, volume 5671, page 248. Springer Science & Business Media, 2009.

[3] N. Balani and S. Ruj. Temporal access control with user revocation for cloud data. In 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014, Beijing, China, September 24-26, 2014, pages 336–343, 2014.

[4] A. Beimel. Secure schemes for secret sharing and key distribution. Ph.D. Thesis, Israel Institute of Technolgy, Technion, Haifa, Israel, 1996.

[5] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA, pages 321–334. IEEE Computer Society, 2007.

[6] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In Proceedings of the 15th ACM conference on Computer and communications security, pages 417–426. ACM, 2008.

[7] R. Canetti, H. Krawczyk, and J. B. Nielsen. Relaxing chosen-ciphertext security. In D. Boneh, editor, Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, volume 2729 of Lecture Notes in Computer Science, pages 565–582. Springer, 2003.

[8] M. Chase. Multi-authority attribute based encryption. In Proceedings of Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007 [8], pages 515–534.

[9] M. Chase and S. S. M. Chow. Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 9-13, 2009 [9], pages 121–130.

[10] CryptoExperts. ABC4Trust. https://www.cryptoexperts.com/research/ projects/abc4trust/. Accessed: 2015-03-28.

[11] S. J. De and S. Ruj. Decentralized access control on data in the cloud with fast encryption and outsourced decryption. In 2015 IEEE Global Communications Conference, GLOBECOM 2015, San Diego, CA, USA, December 6-10, 2015, pages 1–6, 2015.

[12] S. Even, O. Goldreich, and S. Micali. On-line/off-line digital signatures. J. Cryptology, 9(1):35–67, 1996.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. D. C. di Vimercati, editors, Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006, pages 89–98. ACM, 2006.

[14] M. Green, S. Hohenberger, and B. Waters. Outsourcing the decryption of ABE ciphertexts. In 20th USENIX Security Symposium, San Francisco, CA, USA, August 8-12, 2011, Proceedings, 2011.

[15] F. Guo, Y. Mu, and Z. Chen. Identity-based online/offline encryption. In Financial Cryptography and Data Security, 12th International Conference, FC 2008, Cozumel, Mexico, January 28-31, 2008, Revised Selected Papers, pages 247–261, 2008.