Efficient Key Management Protocol for Data Sharing In Cloud

Satwik Deshmukh[1] Vijay Panhalkar[2] Suraj Supekar[3] Shubham Jadham[4]
[1,2,3,4]Siddhant Collage of Engineering, Sudumbre, India

Abstract— Cipher text policy attribute-based cryptography (CP-ABE) is also a promising science technique for fine grained access management of outsourced information at intervals the cloud. However, some drawbacks of key management hinder the popularity of its application. One drawback in imperative need of resolution is that the key official document downside. We've got an inclination to point that front-end devices of shoppers likewise phones usually have restricted privacy protection, thus if personal keys square measure entirely management by them, shoppers risk key exposure that is hardly detected but inherently existed in previous analysis. Moreover, monumental client coding overhead limits the wise use of ABE. Throughout this work, we've got an inclination to propose a cooperative key management protocol in CP-ABE (CKM-CP-ABE). Our construction realizes distributed generation, issue and storage of private keys whereas not adding any extra infrastructure. A fine-grained and immediate attribute revocation is provided for key update. The projected cooperative mechanism effectively solves not entirely key official document downside but jointly key exposure. Meanwhile, it helps markedly cut back client coding overhead. A comparison with completely different representative CP-ABE themes demonstrates that our theme has somewhat higher performance in terms of cloud-based outsourced information sharing on mobile devices. Finally, we provide proof of security for the projected protocol.

Key words: Cloud Data Sharing, CP-ABE, Key Management, Security, Efficiency

I. INTRODUCTION

With cost-effectiveness enhancements in procedure technology and massive scale networks, sharing info with others becomes correspondingly further convenient. Additionally, digital resources are further merely obtained via cloud computing and storage. Since cloud info sharing desires off-premises infrastructure that some organizations put together command, remote storage are somehow threatening privacy of data householders. Therefore, imposing the protection of personal, confidential associated sensitive info keep at intervals the cloud is extremely crucial the coincidental participation of an oversize vary of user's desires fine grained access management for info sharing. Attribute based secret writing (ABE) could also be a promising crypto logical primitive that gives an interesting resolution to secure and versatile info sharing. ABE has associate inherent one-to-many property, which means one key can decipher utterly different cipher texts or different keys can decipher identical cipher text. There unit a pair of types of ABE, referred to as cipher text policy ABE (CP-ABE) and key policy ABE (KP ABE). For CP-ABE, the access policy is embedded into a cipher text and additionally the attribute set is embedded into a personal key. For KP-ABE, the access policy is embedded into a personal key and additionally the attribute set is embedded into a cipher text. CP-ABE permits data householders to stipulate their own access policy. Anyone World Health Organization must get data must initial match the access policy attribute set. Thanks to this property, CP-ABE is kind of applicable for the event of secure, fine-grained access management for cloud data sharing ABE comes in a pair of flavors referred to as key-policy ABE (KP-ABE) and cipher text-policy. In KP-ABE, attributes are accustomed describe the encrypted information and policies are designed into users keys; whereas in CP-ABE, the attributes are accustomed describe a user's certification, associated an cipher or determines a policy on World Health Organization will decode the information.

II. LITERATURE SURVEY

Cipher text policy attribute-based encryption (CP-ABE) is a promising cryptographic technique for fine-grained access control of outsourced data in the cloud. However, some drawbacks of key management hinder the popularity of its application. One drawback in urgent need of solution is the key escrow problem. We indicate that front-end devices of clients like smart phones generally have limited privacy protection, so if private keys are entirely held by them, clients risk key exposure that is hardly noticed but inherently existed in previous research. Furthermore, enormous client decryption overhead limits the practical use of ABE. In this work, we propose a collaborative key management protocol in CP-ABE (CKM-CP-ABE). Our construction realizes distributed generation, issue and storage of private keys without adding any extra infrastructure. A fine-grained and immediate attribute revocation is provided for key update. The proposed collaborative mechanism effectively solves not only key escrow problem but also key exposure. Meanwhile, it helps markedly reduce client decryption overhead. A comparison with other representative CP-ABE schemes demonstrates that our scheme has somewhat better performance in terms of cloud-based outsourced data sharing on mobile devices. Finally, we provide proof of security for the proposed protocol [1].

A Fuzzy IBE theme will be applied to modify coding exploitation biometric inputs as identities; the error-tolerance property of a Fuzzy IBE theme is exactly what permits for the employment of biometric identities that inherently can have some noise every time they're sampled. To boot, we tend to show that Fuzzy-IBE will be used for a kind of application that we tend to term "attribute-based encryption". During this paper we tend to gift 2 constructions of Fuzzy IBE schemes. Our constructions will be viewed as associate Identity-Based coding of a message below many attributes that compose a (fuzzy) identity. Our IBE schemes are each error-tolerant and secure against collusion attacks. To boot, our basic construction doesn't use random oracles. We tend to prove the safety of our schemes below the Selective-ID security model [2].

We develop a brand new cryptosystem for fine-grained sharing of encrypted information that we tend to decision Key-Policy Attribute-Based coding (KP-ABE). In our cryptosystem, cipher texts are labeled with sets of

attributes and personal keys are related to access structures that management that cipher texts a user is ready to decode. We tend to demonstrate the relevance of our construction to sharing of audit-log info and broadcast coding. Our construction supports delegation of personal keys that subsumes graded Identity-Based coding (HIBE). In our system, Fine-grained access management systems facilitate granting access rights to a collection of users and permit exibility in specifying the access rights of individual users. Many techniques are renowned for implementing fine grained access management [3].

Attribute-Based Access management with economical Revocation in information Outsourcing Systems. In this paper, we tend to propose associate access management mechanism exploitation cipher text-policy attribute- based mostly coding to enforce access management policies with economical attribute and user revocation capability. The fine-grained access management will be achieved by twin coding mechanism that takes advantage of the attribute-based coding and selective cluster key distribution in every attribute cluster. We tend to demonstrate a way to apply the projected mechanism to firmly manage the outsourced information. The analysis results indicate that the projected theme is economical and secure within the information outsourcing systems. ABE comes in 2flavors referred to as key-policy ABE (KP-ABE) and cipher text-policy ABE [4].

During this paper, we tend to study CP-ABE schemes within which access structures are AND gates on positive and negative attributes. Our basic theme is tested to be chosen plaintext (CPA) secure below the decisional additive Diffie-Hellman (DBDH) assumption. We tend to then apply the Canetti-Halevi-Katz technique to get a selected cipher text (CCA) secure extension exploitation one-time signatures. The safety proof could be a reduction to the DBDH assumption and therefore the sturdy existential unforgeability of the signature primitive [5].

In our most efficient system, cipher text size, encryption, and secret writing time scales linearly with the complexness of the access formula. The sole previous work to realize these parameters was restricted to a signal within the generic cluster model. We tend to gift 3 constructions at intervals our framework. Our system is tested by selection secure below an assumption that we tend to decision the decisional Parallel additive Diffle -Hellman Exponent (PBDHE) assumption which may be viewed as a generalization of the BDHE assumption [8].

III. EXISTING SYSTEM

Cipher text policy attribute-based secret writing (CP-ABE) may be a promising scientific discipline branch of technique for fine-grained access management of outsourced knowledge at intervals the cloud. However, some drawbacks of key management hinder the popularity of its application. One disadvantage in pressing need of resolution is that the key understanding draws back. We a bent to point that front-end devices of purchasers like sensible phones sometimes have restricted privacy protection, so if personal keys unit entirely management by them, purchasers risk key exposure that is hardly noticed but inherently existed in previous analysis. What's a lot of, monumental shopper cryptography overhead limits the smart use of Attribute based totally secret writing. Previous schemes of key management in attribute based data sharing system primarily focuses on key update, proxy re-encryption and outsourced cryptography. Some analysis incontestable untrusted key authority may end in key understanding draw back and provided corresponding solutions.

A. Existing System Disadvantages

1) One drawback is the key escrow problem.
2) Key authority must be completely trustworthy, as it can decrypt all the cipher text using a generated private key without permission of its owner.

IV. OBJECTIVE

1) Attribute based data sharing.
2) Data stored in encrypted format to improve privacy.
3) Collaborative key management for resolving key escrow problem.
4) Well defined access structure for improve security.

V. PROPOSED SYSTEM

Propose a totally distinctive cooperative key management protocol in cipher text policy attribute-based coding (CKM-CP-ABE) about to enhance security and efficiency of key management in cloud data sharing system. The foremost contributions unit summarized we tend to introduce attribute groups to form the private key update formula. A singular attribute cluster secret is assigned to each attribute cluster that contains purchasers World Health Organization share identical attribute. Via modification attribute cluster key, a fine-grained and immediate attribute revocation is provided. We tend to tend to point that not exclusively key understanding downside but together key exposure is threatening the confidentiality of private keys, that's hardly detected in previous analysis. Compared to previous key management protocols for attribute-based data sharing system in cloud, our planned protocol effectively addresses every a pair of problems by its cooperative key management. Finally, we provide proof of security for the planned protocol. The cooperative mechanisms helps markedly decrease shopper decryption overhead by employing a decryption server to execute most of decryption whereas leave no info relating to information to it.

A. Proposed System Advantages

1) In proposed system, novel collaborative protocol is presented. With help of interaction among the key authority, a cloud server and client who tends to access data, we resolve the key escrow problem.
2) Resolve Key exposure problem.

VI. ALGORITHMS

A. Algorithm 1: AES Algorithm

1) Algorithm Steps

Step 1: Start
Step 2: Derive the set of round keys from the cipher key.

Step 3: Initialize the state array with the block data (plaintext).
Step 4: Add the initial round key to the starting state array.
Step 5: Add the initial round key to the starting state array.
Step 6: Perform the tenth and final round of state manipulation.
Step 7: Copy the final state array out as the encrypted data (cipher text).

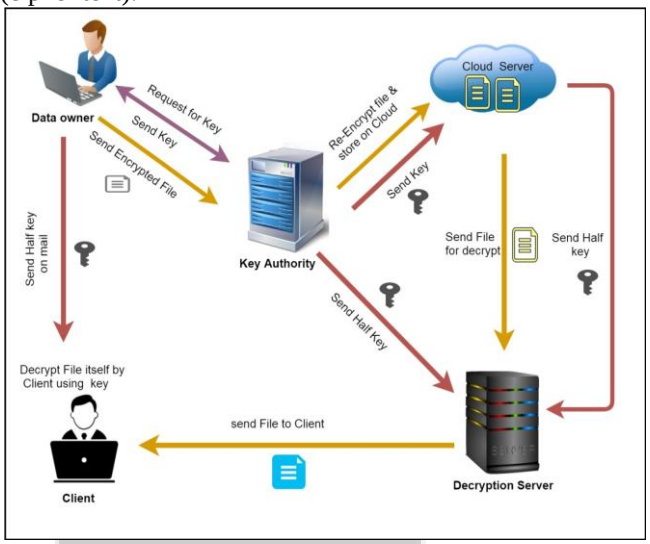

Fig. 1:

B. System Requirement and Specification

1) Hardware Resources Required

1) Processor Pentium –IV
2) Speed: 1.1 GHz
3) RAM: 256 MB (min)
4) Hard Disk: 20 GB
5) Key Board: Standard Windows Keyboard
6) Mouse: Two or Three Button Mouse
7) Monitor: SVGA

C. Software Resources Required

1) Operating System: Windows 07/08/Above
2) Programming Language: JAVA/J2EE/XML
3) Database: MY SQL

VII. Conclusion and Future Scope

The projected cooperative mechanism dead addresses not solely key written agreement downside however additionally a worse downside referred to as key exposure that previous analysis hardly noticed. Meantime it helps to optimize clients' user expertise since solely little quantity of responsibility is taken by them for secret writing. Thus, the projected theme performs higher in cloud information sharing system serving huge performance-restrained front-end devices with regard to either security or potency.

Acknowledgements

This work is supported by Prof. Subhash Patel (Siddhant College of Engineering)

References

[1] A Collaborative Key Management Protocol in Cipher text Policy Attribute-Based Encryption for Cloud DataSharing.
[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. EuroCrypt, 2005, pp. 457-473.
[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc.ACM CCS, 2006, pp. 89-98.
[4] L. Cheung, and C. Newport, "Provably secure cipher text policy ABE," inProc. ACM CCS, 2007, pp. 456-465.
[5] J. Bethencourt, A. Sahai, and B.Waters, "Cipher text-policy attribute-based encryption," in Proc. IEEE Symp. Secure. Privacy, 2007, pp. 321-334.
[6] J. Hur, and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214-1221, 2011.
[7] B. Waters, "Cipher text-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography, 2011, pp. 53-70.
[8] M. Green, S. Hohnberger, and B. Waters, "Outsourcing the decryption of ABE cipher text," in Proc. USENIX Secur. Symp. 2011, pp. 34.
[9] P. P. Chandra, D. Mutkurman, and M. Rathinrai, "Hierarchical attribute based proxy encryption access control in cloud computing," in Proc.ICCPCT, 2014, pp. 1565-1570.
[10] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forens. Security, vol. 8, no. 8, pp. 1343-1354, 2013.
[11] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forens. Security, vol. 10, no. 10, pp. 2119-2130, 2015.

