A NOVEL APPROACH FOR KEYWORD SEARCH OVER ENCRYPTED CLOUD DATA USING ABE ALGORITHM

MANDHADAPU HARITHA, MCA, DCA,

DVR & Dr.HS MIC College of Technology, A.P., India.

MARESWARAMMA. P, Assistant Professor, Dept.of AI & IT,

DVR & Dr.HS MIC College of Technology, A.P., India.

ABSTRACT:

He problem of keyword search with access control over encrypted data in cloud computing which enables Keyword Search with Access Control over encrypted data. Leveraging Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) scheme can achieve keyword-based retrieval and fine-grained access control simultaneously. However, the single attribute authority in existing CP-ABKS schemes is tasked with costly user certificate verification and secret key distribution. In addition, this results in a single-point performance bottleneck in distributed cloud systems. Thus, in this paper, we present a secure Multi-authority CP-ABKS (MABKS) system to address such limitations and minimize the computation and storage burden on resource-limited devices in cloud systems. In addition, the MABKS system is extended to support malicious attribute authority tracing and attribute update. Our rigorous security analysis shows that the MABKS system is selectively secure in both selective-matrix and selective-attribute models. Our experimental results using real-world datasets demonstrate the efficiency and utility of the MABKS system in practical applications.

INTRODUCTION

Searchable Encryption (SE) is an important technique to guarantee data security and usability in the cloud at the same time. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams.

Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

LITERATURE SURVEY

Expressive, efficient and revocable data access control for multi-authority cloud storage

AUTHORS: K. Yang and X. Jia

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

Privacy preserving cloud data access with multi-authorities

AUTHORS: T. Jung, X. Li, Z. Wan, and M. Wan

Cloud computing is a revolutionary computing paradigm which enables flexible, on-demand and low-cost usage of computing resources. Those advantages, ironically, are the causes of security and privacy problems, which emerge because the data owned by different users are stored in some cloud servers instead of under their own control. To deal with security problems, various schemes based on the Attribute-Based Encryption have been proposed recently. However, the privacy problem of cloud computing is yet to be solved. This paper presents an anonymous privilege control scheme AnonyControl to address not only the data privacy problem in a cloud storage, but also the user identity privacy issues in existing access control schemes. By using multiple authorities in cloud computing system, our proposed scheme achieves anonymous cloud data access and fine-grained privilege control. Our security proof and performance analysis shows that AnonyControl is both secure and efficient for cloud computing environment.

PROBLEM DEFINITION

In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t; n) threshold secret sharing into our scheme to share the secret key among authorities. In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key.

PROPOSED SYSTEM

- To the best of our knowledge, we are the first to design a multi-authority access control architecture to deal with the problem.
- By introducing the combining of (t; n) threshold secret sharing and multi-authority CP-ABE scheme, we propose and realize a robust and verifiable multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set.
- Furthermore, by efficiently combining the traditional multi-authority scheme with ours, we construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

PROPOSED METHOD

• ***Multi-authority architecture.*** Different from the previous single-authority CP-ABKS schemes (or traditional multi-authority CP-ABE schemes) that still cannot avoid the limitation of single-point performance bottleneck, the hierarchical structure in the MABKS system enables multiple AAs to separately execute time-consuming user certificate verification and intermediate secret key generation on behalf of CA, which significantly reduces CA's computation requirements.

• ***File-level fine-grained keyword search.*** Most of the traditional CP-ABKS schemes have independent file key encryption and indexes building processes, while the MABKS system will embed the secret key chosen in file key encryption process into the indexes building process. Thus, the MABKS system not only allows data owners to specify the file-level fine-grained access control over encrypted cloud data but also enables cloud clients (e.g., data owners, data users) to perform keyword-based ciphertexts retrieval.

• ***Malicious AAs tracing.*** The traditional traceable CPABE schemes mainly focus on the malicious data users who may leak their secret keys to unauthorized entities, while the extended MABKS system focuses on tracing the malicious AAs that incorrectly generate intermediate secret keys for data users in two phases (i.e., secret key ownership confirming, malicious AAs tracing).

• ***Attribute update.*** The extended MABKS system implements the attribute update so that malicious data users cannot access the sensitive cloud data by exploiting old or outdated secret keys. Compared with the attribute update mechanisms in prior CP-ABE schemes that need to update the whole ciphertexts, the extended MABKS just allows data users and cloud server to update a fraction of secret key components and indexes associated with the updated attributes by using two transformation keys,respectively.

• ***Security and efficiency***. The comprehensive security analysis shows that the MABKS system is selectively secure in both selective-matrix and selective attribute models. Experimental results using real world datasets demonstrate that the storage and computation overhead increases with the number of user attributes rather than system attributes. In addition, the MABKS system has constant trapdoor size and ciphertexts retrieval overhead, which reduces the storage and computation burden on resource-limited data users and improves the user search experience. Considering that the encryption and decryption overhead still grows with the complexities of access policies in traditional CP-ABKS schemes, the MABKS system can utilize the online/offline encryption mechanism and outsourced decryption mechanism to further decrease the data owner and data users' computation overhead, respectively.

Advantages:

- The security model of the MABKS system allows a certain adversary to query for the secret key which cannot be utilized to decrypt the challenging cipher texts.
- Traditional CP-ABKS schemes that can achieve fine-grained access control and keyword-based cipher texts retrieval at the same time by simply combining CP-ABE and SE techniques, the MABKS system can gain the file-level fine grained key

IMPLEMENTATION

The System Design Document describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces.

- TMACS
- Data Access Control Scheme
- Certificate authority
- Attribute authorities

MODULES DESCRIPTION

TMACS:

The TMACS multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. In TMACS, a global certificate authority is responsible for the construction of the system, which avoids the extra overhead caused by AAs' negotiation of system parameters. CA is also responsible for the registration of users, which avoids AAs synchronized maintaining a list of users. However, CA is not involved in AAs' master key sharing and users' secret key generation, which avoids CA becoming the security vulnerability and performance bottleneck.design of TMACS is reusing of the master key shared among multiple attribute authorities. In traditional (t;n) threshold secret sharing, once the secret is reconstructed among multiple participants, someone can actually gain its value. Similarly, in CP-ABE schemes, the only-one-authority knows the master key and uses it to generate each user's secret key according to a specific attribute set. In this case, if the AA is compromised by an adversary, it will become the security vulnerability. To avoid this, by means of (t;n) threshold secret sharing, the master key cannot be individually reconstructed and gained by any entity in TMACS.hat the master key a is actually secure. By this means, we solve the problem of reusing of the master key.

Data Access Control Scheme:

we propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes. In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t;n) threshold secret sharing into our scheme to share the secret key among authorities. In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t;n) threshold secret sharing guarantees that the master key cannot be obtained by any authorityalone. TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. To the best of our knowledge, this paper is the first try to address the singlepoint bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

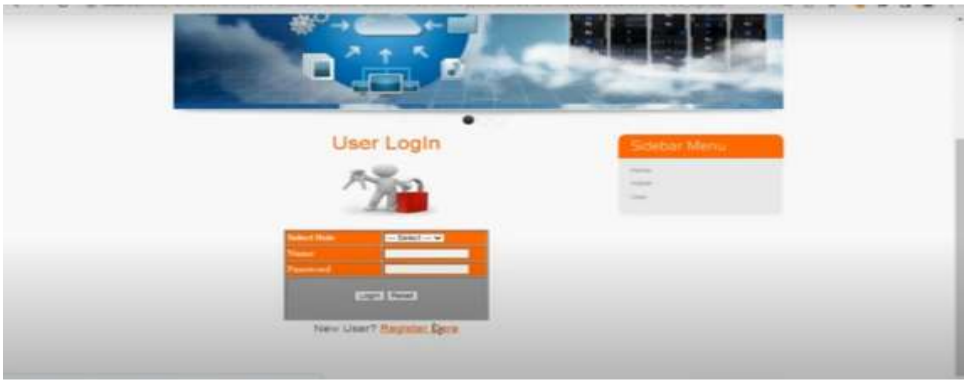
Certificate authority:

The certificate authority is a global trusted entity in the system that is responsible for the construction of the system by setting up system parameters and attribute public key (PK) of each attribute in the whole attribute set. CA accepts users and AAs' registration requests by assigning a unique uid for each legal user and a unique aid for each AA. CA also decides the parameter t about the threshold of AAs that are involved in users' secret key generation for each time. However, CA is not involved in AAs' master key sharing and users' secret key generation. Therefore, for example, CA can be government organizations or enterprise departments which are responsible for the registration. certificate authority is responsible for the construction of the system, which avoids the extra overhead caused by AAs' negotiation of system parameters. CA is also responsible for the registration of users, which avoids AAs synchronized maintaining a list of users.

Attribute authorities:

The attribute authorities focus on the task of attribute management and key generation. Besides, AAs take part of the responsibility to construct the system, and they can be the administrators or the managers of the application system. Different from other existing multi-authority CP-ABE systems, all AAs jointly manage the whole attribute set, however, any one of AAs cannot assign users' secret keys alone for the master key is shared by all AAs. All AAs cooperate with each other to share the master key. By this means, each AA can gain a piece of master key shareas its private key, then each AA sends its corresponding public key to CA to generate one of the system public keys. When it comes to generate users' secret key, each AA only should generate its corresponding secret key independently. the master key shared among multiple attribute authorities. In traditional (t;n) threshold secret sharing, once the secret is reconstructed among multiple participants, someone can actually gain its value.

SAMPLE RESULTS



CONCLUSION

In this paper, we proposed an efficient and feasible MABKS system to support multiple authorities, in order to avoid having performance bottleneck at a single point in cloud systems. Furthermore, the presented MABKS system allows us to trace malicious AAs (e.g., to prevent collusion attacks) and support attribute update (e.g., to avoid unauthorized access using outdated secret keys). We then demonstrated the selective security level of the system in selective-matrix and selective-attribute models under decisional q-parallel BDHE and DBDH assumptions, respectively. We also evaluated the system's performance and demonstrated that significant computation and storage cost reductions were achieved, in comparison to prior ABKS schemes. However, the main flaw is that the MABKS system cannot support expressive search queries such as conjunctive keyword search, fuzzy search, subset search and so on. The future work will focus on building an efficient and flexible index construction so that the MABKS system is capable of supporting various search requests.

BIBILIOGRAPHY

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat. Instit.Standards Technol., vol. 53, no. 6, p. 50, 2009.

[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Proc. 14th Financial Cryptography Data Security, 2010, pp. 136–149.

[3] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan.-Feb.2012.

[4] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 457–473.

[5] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in Proc. 14th ACM Conf. Comput.Commun. Security, 2014, pp. 195–203.

[6] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in Proc. 29th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2010, pp. 62–91.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[8] N. Attrapadung, B. Libert, and E. Panafieu, “Expressive keypolicy attribute-based encryption with constant-size ciphertexts,” in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography, 2011, pp. 90–108.

[9] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[10] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography, 2011, pp. 53–70.

[11] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded ciphertext policy attribute based encryption,” in Proc. 35th Int. Colloquium Automata, Lang. Programm., 2008, pp. 579–591.

[12] R. Bobba, H. Khurana, and M. Prabhakaran, “Attribute-sets: A practically motivated enhancement to attribute-based encryption,” in Proc. 14th Eur. Symp. Res. Comput. Security, 2009, pp. 587–604.