www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Securing data in the image using SHA&ECC

[1]Mr. SITARAM CHILAKAPATI , [2]MALLELA SIREESHA, [3]PODAMAKALA. UDAYA LAKSHMI, [4]PONUGOTI SRILEKHA, [5]MARRIPUDI MANASA
[1](Assistant Professor), CSE, RISE Krishna Sai Gandhi Group of Institutions Ongole
[2345]B.TECH, scholar, CSE, RISE Krishna Sai Gandhi Group of Institutions Ongole

ABSTRACT

In today's digital age, the need for secure data transmission and storage has never been more critical. Images, which often carry sensitive information, are frequently shared over the internet, making them vulnerable to tampering and unauthorized access. This paper proposes a novel approach for securing data within images using the combination of Secure Hash Algorithm (SHA) and Elliptic Curve Cryptography (ECC). The proposed system embeds secret data within the image using SHA to generate a unique hash, ensuring data integrity, while ECC is employed to encrypt the hash, providing confidentiality. This hybrid method offers enhanced security compared to traditional techniques by ensuring both the protection of the data and the image's integrity. The system can be particularly useful for applications in secure communication, digital watermarking, and protecting intellectual property.

KEYWORDS: Data security, image encryption, SHA, ECC, data integrity, elliptic curve cryptography, secure hash algorithm, digital watermarking, image processing, cryptography.

1.INTRODUCTION

THE prevalence of cloud computing may indirectly incur vulnerability to the confidentiality of outsourced data and the privacy of cloud users. A particular challenge here is on how to guarantee that only authorized users can gain access to the data, which has been outsourced to cloud, at anywhere and anytime. One naive solution is to employ encryption technique on the data prior to uploading to cloud. However, the solution limits further data sharing and processing. This is so because a data owner needs to download the encrypted data from cloud and further re-encrypt them for sharing (suppose the data owner has no local copies of the data). A fine-grained access control over encrypted data is desirable in the context of cloud computing .Ciphertext-Policy Attribute-Based Encryption (CPABE)may be an effective solution to guarantee the confidentiality of data and provide fine-grained access control here. In a CP-ABE based cloud storage system, for example, organizations (e.g., a university such as the University of Texas at SanAntonio) and individuals(e.g.,students,facultymembers and visiting scholars of the university) can first specify access policy over attributes of a potential cloud user.Authorized cloud users the nare granted access credentials (i.e., decryption keys) corresponding to their attribute sets (e.g., student role, faculty member role, or visitor role), which can be used to obtain access to the outsourced data. As a robust one-to-many encryption mechanism, CP-ABE offers a reliable method to protect data stored in cloud, but also enables fine-grained access control over the data. Generally speaking, the existing CP-ABE based cloud storage systems fail to consider the case where access credential is misused. For instance, a university deploys a CPABE based cloud storage system to outsource encrypted student data to cloud under some access policies that are compliant with the relevant data sharing and privacy legislation (e.g., the federal Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act of 1992 (HIPAA)). The official in charge at the organization (e.g. university's security manager) initializes the system parameters and issues access credentials for all users (e.g., students, faculty members, and visiting scholars). Each employee is assigned with several attributes (e.g.,"administrator","seniormanager","financialofficer", "tenured faculty", "tenure-track faculty", "non tenure-track faculty", "instructors", "adjunct", "visitor", and/or "students"). Only the employees with attributes satisfying the decryption policy of the outsourced data are able to gain access to the student data stored in cloud (e.g. student admission materials). As we may have known, the leakage of any sensitive student information stored in cloud could result in a range of consequences for the organization and individuals (e.g., litigation, loss of competitive advantage, and criminal charges). The CP-ABE may help us prevent security breach from outside attackers. But when an insider of the organization is suspected to commit the “crimes” related to the redistribution of decryption rights and the circulation of student information in plain format for illicit financial Is it also possible for us to revoke the compromised access privileges? In addition to the above questions, we have one more which is related to key generation authority. A cloud user’s access credential (i.e., decryption key) is usually issued by a semi-trusted authority based on the attributes the user possesses. How could we guarantee that this particular authority will not (re-)distribute the generated access credentials to others? For example, the organization security official leaks a lecturer Alice’s key to an outsider Bob (who is not the employee of the university). One potential answer to the question is to employ multiple authorities. Nevertheless, this incurs additional cost in communication and infrastructure deployment and meanwhile, the problem of malicious collusion among authorities remains. Therefore, we posit that adopting an accountable authority approach to mitigate the access credential escrow problem is the preferred strategy. Seeking to mitigate access credential misuse, we propose Crypt Cloud+, an accountable authority and revocable CPABE based cloud storage system with white-boxtraceability and auditing. To the best of our knowledge, this is the first practical solution to secure fine-grained access control over encrypted data in cloud. Specifically, in our work, we first present a CP-ABE based cloud storage framework. Using this (generic) framework, we propose two accountable authority and revocable CP-ABE systems (with whitebox traceability and auditing) that are fully secure in the standardmodel,referredtoasATER-CP-ABEandATIR-CPABE, respectively. Based on the two systems, we present the construction of CryptCloud+ that provides the following features. 1) Traceability of malicious cloud users. Users who leak their access credentials can be traced and identified. 2) Accountable authority. A semi-trusted authority, who (without proper authorization) generates and further distributes access credentials to unauthorized user(s), can be identified. This allows further actions to be undertaken (e.g. criminal investigation or civil litigation for damages and breach of contract). 3) Auditing. An auditor can determine if a (suspected) cloud user is guilty in leaking his/her access credential. 4) “Almost” zero storage requirement for tracing. We use a Paillier-like encryption as an extract able commitment in tracing malicious cloud users and more practically, we do not need to maintain an identity table of users for tracing Malicious cloud users revocation. Access credentials for individual traced and further determined to be "compromised" can be revoked. We design two mechanisms to revoke the "traitor(s)" effectively. The ATER-CP-ABE provides an explicitly revocation mechanism where a revocation list is specified explicitly into the algorithm Encrypt, while the ATIRCP-ABE offers an implicitly revocation where the encryption does not need to know the revocation list but a key update operation is required periodically. This paper extends our earlier work as follows.

1) We present a formal framework model of the proposed system, designed for practical cloud storage system deployment.

2) We address a weakness in the auditing procedure of the conference version. Specifically, a malicious user may change tid of his secret key in the conference version, and the auditing procedure will fail in this case. As a mitigation, we revise the key generation algorithm and add an audit list to detect if the tid is changed.

3) We enhance the functionality of the construction (w.r.t. AAT-CP-ABE) proposed in the conference version and further present two enhanced constructions, namely ATER-CP-ABE and ATIR-CP-ABE. These constructions allow us to effectively revoke the malicious users explicitly or implicitly. We also present the new definitions, technique and related materials of ATER-CP-ABE and ATIR-CP-ABE.

4) Based on the new ATER-CP-ABE and ATIR-CPABE, we present CryptCloud+ which is an effective and practical solution for secure cloud storage.

5) We provide general extensions (of our system) on the large universe, the multi-use, and the prime-order setting cases, so that the solution introduced in this paper is more scalable in real-world applications.

6) We comprehensively evaluate the efficiency of the proposed ATER-CP-ABE and ATIR-CP-ABE via experiments.

2. EXISTING SYSTEM

Li et al. introduce the notion of accountable CP-ABE [23] to prevent unauthorized key distribution among colluded users. In a later work [22], a user accountable multi-authority CP-ABE system is proposed. Liu et al. also proposed white-box [27] and black-box [26] traceability 1 CP-ABE systems supporting policy expressiveness in any monotone access structures.

Ning et al. [30], [32], [34], [36] propose several practical CP-ABE systems with white-box traceability and black-box traceability. Deng et al. [11] provide a tracing mechanism of CP-ABE to find the leaked access credentials in cloud storage system.

Sahai et al. [40] define the problem of revocable storage and provide a fully secure construction for ABE based on ciphertext delegation. Yang et al. [49] propose a revocable multi-authority CP-ABE system that achieves both forward and backward security. More recently, Yang et al. [50] propose an attribute updating method to achieve the dynamic change on attribute (such as revoking previous attribute and re-granting previously revoked attribute).

Advantages

- Traceability of malicious cloud users. Users who leak their access credentials can be traced and identified.
- Accountable authority. A semi-trusted authority, who (without proper authorization) generates and further distributes access credentials to unauthorized user(s), can bZidentified. This allows further actions to be undertaken (e.g. criminal investigation or civil litigation for damages and breach of contract).

Auditing. An auditor can determine if a (suspected) Cloud.

PROPOSED SYSTEM

- The proposed system presents a formal framework model of the proposed system, designed for practical cloud storage system deployment.
- The system addresses a weakness in the auditing procedure of the conference version. Specifically, a malicious user may change tid of his secret key in the conference version, and the auditing procedure will fail in this case. As a mitigation, we revise the key generation algorithm and add an audit list to detect if the tid is changed.
- The system enhances the functionality of the construction (w.r.t. AAT-CP-ABE) proposed in the conference version and further present two enhanced constructions, namely ATER-CP-ABE and ATIR-CP-ABE. These constructions

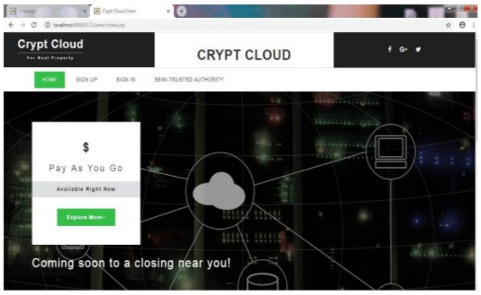
allow us to effectively revoke the malicious users explicitly or implicitly. We also present the new definitions, technique and related materials of ATER-CP-ABE and ATIR-CP-ABE.

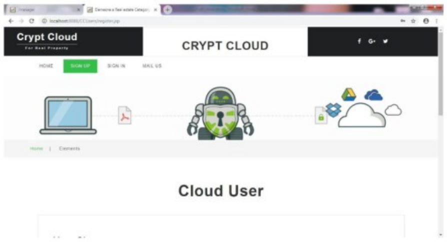
- Based on the new ATER-CP-ABE and ATIR-CPABE, we present CryptCloud+ which is an effective and practical solution for secure cloud storage.
- The system provides general extensions (of our system) on the large universe, the multi-use, and the prime-order setting cases, so that the solution introduced in this paper is more scalable in real-world applications.
- The system comprehensively evaluates the efficiency of the proposed ATER-CP-ABE and ATIR-CP-ABE via experiments.

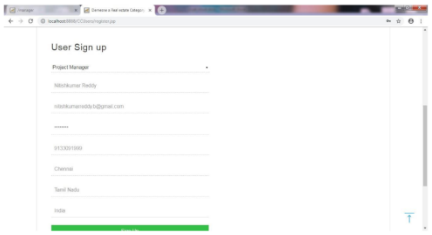
Disadvantages

- There is less security on outsourced data due to lack of Verification Based on Hash code.
- There is no more security in the data
- access.

3. RESULTS






User Sign up

Project Manager

Nitishkumar Reddy

nitishkumarreddy.b@gmail.com

••••••••

9133091999

Chennai

Tamil Nadu

India

4. CONCLUSION

in this work, we have addressed the challenge of credential leakageincp-abebasedcloudstoragesystembydesigning an accountable authority and revocable cryptcloud which supports white-box traceability and auditing (referred to as cryptcloud+). this is the first cp-abe based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. specifically, cryptcloud+ allows us to trace and revoke malicious cloud users (leaking credentials). our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority. we note that we may need black-box traceability, which is a stronger notion (compared to white-box traceability), in cryptcloud. one of our future works is to consider the black-box traceability and auditing. furthermore, au is assumed to be fully trusted in cryptcloud+. however, in practice, it may not be the case. is there any way to reduce trust from au? intuitively, one method is to employ multiple aus.thisis similar to the technique used in threshold schemes. but it will require additional communication and deployment costand meanwhile, the problem of collusion among aus remains. another potential approach is to employ secure multi-party computation in the presence of malicious adversaries. however, the efficiency is also a bottleneck. designing efficient multi-party computation and decentralizing trust among aus (while maintaining the same level of security and efficiency) is also a part of our future work. we use paillier-like encryption to serve as an extractable commitment to achieve white-box traceability. from an abstract view point, any extractable commitment may be employed to achieve white-box traceability in theory. to improve the efficiency of tracing, we may make use of a more light-weight (pairing-suitable) extractable commitment. also, the trace algorithm in cryptcloud+ needs to take the master secret key as input to achieve white-box traceability of malicious cloud users. intuitively, the proposed cryptcloud+ is private traceable5. private traceability only allows the tracing algorithm to be run by the system administrator itself, while partial/full public traceability enables the administrator, authorized users and even anyone without the secret information of the system to fulfill the trace. our future work will include extending cryptcloud+ to provide "partial" and fully public traceability without compromising on performance.

5. REFERENCE

1. Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.

2. Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.

3. Michael Armbrust, Armando Fox, R ean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50– 58, 2010.

4. Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278– 300. Springer, 2009.

5. Amos Beimel. Secure schemes for secret sharingand key distribution. PhD