ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Novel Method for Secure Data Access Control and Exchange Using Error Estimating

P.Mohan Rao
**Dept of Computer Science Engineering,
Andhra University College of Engineering,
Visakhapatnam, AP, India.**

Dr.Kasukurthi Venkata Rao
**Dept of Computer Science Engineering,
Andhra University College of Engineering,
Visakhapatnam, AP, India.**

Abstract:

Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present a semi anonymous privilege control scheme to address not only the data privacy, but also the user identity privacy in existing access control schemes. Decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the system, which fully prevents the identity leakage and achieve the full anonymity. assumption, and our performance evaluation exhibits the feasibility of our schemes.

Keywords:

Cloud Storage, Attribute-Based Encryption, Chiper texts, Scalable Mobile applications.

1. Introduction:

Cloud computing has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [2]. As a disruptive technology with profound implications, cloud computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data are being centralized or outsourced to the cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc., [3]. While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats toward users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity [4]. Examples of outages and security breaches of noteworthy cloud services appear from time to time [5], [6], [7]. Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status. For examples, CSP might reclaim storage for monetary reasons by discarding data that have not been or are rarely accessed, or even hide data loss incidents to maintain a reputation [8], [9], [10]. In short, although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture. This concept comes from a special kind of encryption scheme called deniable encryption, first proposed in [11]. Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in ciphertexts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence. This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data.

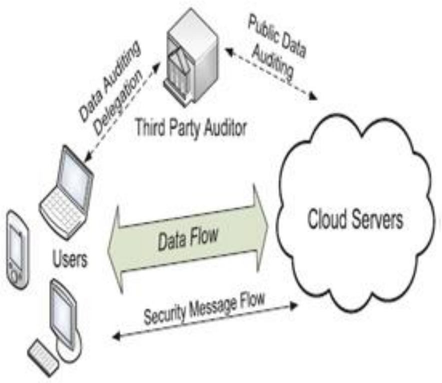

Fig. 1. Architecture of Cloud data storage device

2. Related Work:

The need to store information externally has never been higher: With users and organizations expecting to access and modify information across multiple platforms and geographic locations, there are numerous advantages to storing data in the cloud. However, there is a natural resistance to the idea of handing over sensitive information to external storage. Since these databases are often filled with valuable data, they are high value targets for attackers and security breaches in such systems are not uncommon, especially by insiders. In addition, organizations with access to extremely sensitive data might not want to give an outside server any access to their information at all. Similar problems can easily arise when dealing with centralized storage within a single organization, where different users in different departments have access to varying levels of sensitive data. A first step in addressing this problem of trust is to only store information in encrypted form. However, data access is not static { as employees are hired, fired or promoted, it will be necessary to change who can access certain data. A natural solution to this problem is to have users authenticate their credentials before giving them access to data; but such an approach requires a great deal of trust in the server: a malicious party may be able to penetrate the server and bypass authentication by exploiting software vulnerabilities. A solution that avoids this problem is to use cryptographically enforced access control such as attribute-based encryption (ABE) [12]. However, this fails to address the problem that the credentials of a user may change with time. This problem motivated the study of revocation [5] where a periodic (e.g., nightly) key update would only allow non-revoked users to update their keys to decrypt newly encrypted data. Dynamic credentials in the context of stored data, however, present novel challenges that have not been considered in previous studies on revocation. Originally proposed by Sahai and Waters [12], attribute-based encryption [11, 13, 20] has been an active research area in cryptography in part since it is a primitive with interesting functional applications [10, 5] and can be implemented efficiently [4]. In a key-policy attribute-based encryption (KP-ABE) scheme every secret key is generated with a policy P and cipher texts are generated with a set of attributes U and decryption is only possible if P(U) = True. The parallel notion where cipher texts are associated with policies and keys with sets of attributes is called cipher text-policy attribute-based encryption (CP-ABE). While the problem of delegating a key to a more restrictive key has been considered [11], it is analyzed only in the context of the scheme proposed in the paper. The problem of revocation is also a well studied problem, both for general PKI [16, 2, 7, 9], identity based encryption [5, 14] and attribute-based encryption [22]. At a high level, our revocable storage results can be seen as taking methods from forward secure signatures and encryption [6, 3, 1, 15] which were introduced for key management and applying them to cipher text management by noticing that the key delegation infrastructure can be replicated for the ciphertext through the delegation mechanism we introduce.

3. CP-ABE Scheme:

Deniable encryption schemes may have different properties and we provide an introduction to many of these properties below.

- ad hoc deniability vs. plan-ahead deniability: The former can generate a fake message (from the entire message space) when coerced, whereas the latter requires a predetermined fake message for encryption. Undoubtedly, all bitwise encryption schemes are ad hoc.
- sender-, receiver-, and bi-deniability: The prefix here in each case implies the role that can fool the coercer with convincing fake evidence. In sender-deniable encryption schemes and receiver-deniable schemes, it is assumed that the other entity cannot be coerced. Bi-deniability means both sender and receiver can generate fake evidence to pass third-party coercion.
- full deniability vs. multi-distributional deniability: A fully deniable encryption scheme is one in which there is only one set of algorithms, i.e., a key generation algorithm, an encryption algorithm and so on. Senders, receivers and coercers know this set of algorithms and a sender and a receiver can fool a coercer under this condition. As for multi distributional deniable encryption schemes, there are two sets of algorithms, one being a normal set, while the other is a deniable set. The outputs of algorithms in these two sets are computationally indistinguishable. The normal set of algorithms cannot be used to fool coercers, whereas the deniable set can be used. A sender and a receiver can use the deniable algorithm set, but claim that they use the normal algorithm set to fool coercers.
- interactive encryption vs. non-interactive encryption: The difference between these two types of encryption is that the latter scheme does not need interaction between sender and receiver.

4. Methodology:

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.[1] A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. The concept of attribute-based encryption was first proposed by Amit Sahai and Brent Waters [2] and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters.[3] Recently, several researchers have further proposed Attribute-based encryption with multiple authorities who jointly generate users' private keys. Revocation of users in cryptosystems is a well studied but nontrivial problem. Revocation is even more challenging in attribute-based systems, given that each attribute possibly belongs to multiple different users, whereas in traditional PKI systems public/private key pairs are uniquely associated with a single user. In principle, in an ABE system, attributes, not users or keys, are revoked. Now discuss how the revocation feature can be incorporated.

A simple but constrained solution is to include a time attribute. This solution would require each message to be encrypted with a modified access tree T0, which is constructed by augmenting the original access tree T with an additional time attribute. The time attribute, ζ represents the current 'time period'. Formally, the new access structure T0 is as follows: T0 = (T AND ζ). For example, ζ can be the 'date' attribute whose value changes once every day. It is assumed that each non-revoked user receives his fresh private keys corresponding to the 'date' attribute once everyday directly from the mobile key server MKS (which is the central authority) or via the regional delegates. With a hierarchical access structure, the key delegation property of CP-ABE can be exploited to reduce the dependency on the central authority for issuing the new private keys to all users every time interval. There are significant trade-offs between the extra load incurred by the authority for generating and communicating the new keys to the users and the amount of time that can elapse before a revoked user can be effectively purged. This above solution has the following problems:

- Each user X needs to periodically receive from the central authority the fresh private key corresponding to the time attribute, otherwise X will not be able to decrypt any message.
- It is a lazy revocation technique the revoked user is not purged from the system until the current time period expires.
- This scheme requires an implicit time synchronization (a loose time synchronization may be sufficient) among the authority and the users.

In present days data accessing in cloud storage security is the hard task. Due more scalability and increase in data sharing increases the data corruption and network disturbance. It is mainly due to the fake users or intruders in the network. Then researchers introduced Attribute based Encryption, the highest version of the identity based Encryption. It mainly defends on the un-authorization of the users. But it didn't check the message correctness. So we introduced a novel technique of both message correctness and user authentication. It reduces the data corruption and the impersonation attacks. In our work introduced error correction with user authentication. There are some cases, consider that user private details are captured by the intruder. He communicates with the cloud service provider with original user credentials. Then cloud verifies him as original user and shares the information with fake user. Here based on the only authentication service cannot decide that the communicated user is correct user. So we introduced a novel framework for both authentication and the message correctness. Initial setup, User register in cloud service provider and the cloud service provider grants a unique code for user. Rijndael is the block cipher algorithm recently chosen by the National Institute of Science and Technology (NIST) as the Advanced Encryption Standard (AES). It supersedes the Data Encryption Standard (DES). NIST selected Rijndael as the standard symmetric key encryption algorithm to be used to encrypt sensitive (unclassified) American federal information. The choice was based on a careful and comprehensive analysis of the security and efficiency characteristics of Rijndael's algorithm. Rijndael is an iterated block cipher. Therefore, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function). Section 3 provides the details of the Rijndael round function. Rijndael also defines a method to generate a series of subkeys from the original key. The generated subkeys are used as input with the round function. Rijndael was developed by Belgian cryptographers Joan Daemen of Proton World International and Vincent Rijmen of Kathlieke Universite it Leuven [2]. The algorithm that they developed was designed as an easily understandable mathematical structure that can be broken down into simple components. Daemen and Rijmen write in their proposal to AES that Rijndael was designed based on the following three criteria [6].

- Resistance against all known attacks;

- Speed and code compactness on a wide range of platforms;
- Design simplicity

Rijndael was evaluated based on its security, its cost and its algorithm and implementation characteristics. The primary focus of the analysis was on the cipher's security, but the choice of Rijndael was based on its simple algorithm and implementation characteristics. There were several candidate algorithms but Rijndael was selected because based on the analyses, it had the best combination of security, performance, efficiency, ease of implementation and flexibility.

5. Results:

The below figure 2 shows the input data is converted to chiper form and generates code which is an error estimating code. After all this it proves final error estimation for the input data.

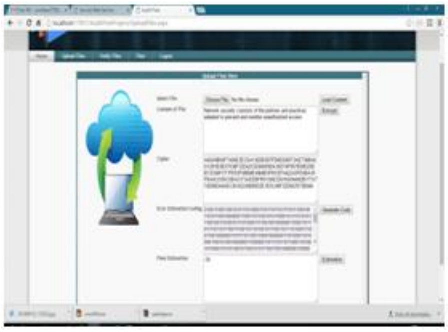

Fig 2. Uploading the input data

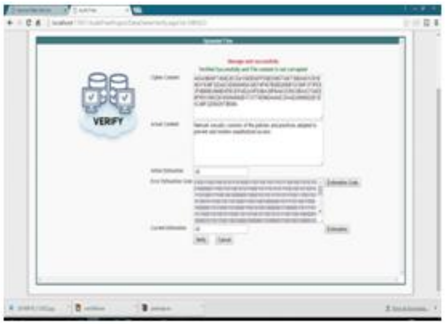

Fig 3. Verifying the file

Figure 3 shows the conversion of the input data at the destination end. The data will appear corrected if the estimated error value is given perfectly. Hence the data will be verified.

6. Conclusion:

In this paper we proposed framework, that combines with cryptographic properties with secure storage. Our framework introduces secure data auditing for multiple owners and secure data verification of multiple files. By using our protocol auditing process can be done in less amount of time. It supports more scalability of users. This contains secure public tags and verification process such as auditing. It reduces work load to server because simple verification process is only done by server all other security issued can done by auditing. Furthermore, our auditing scheme incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server.

References:

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,” Proc. IEEE INFOCOM ’10, Mar. 2010.

[2] P. Mell and T. Grance, “Draft NIST Working Definition of Cloud Computing,” http://csrc.nist.gov/groups/SNS/cloudcomputing/ index.html, June 2009.

[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the Clouds: A Berkeley View of Cloud Computing,” Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[4] Cloud Security Alliance, “Top Threats to Cloud Computing,” http://www.cloudsecurityalliance.org, 2010.

[5] M. Arrington,“Gmail Disaster: Reports of Mass Email Deletions, http://www.techcrunch.com/2006/12/28/ gmail disaster reports of- mass-email-deletions/, 2006.

[6] J. Kincaid, “Media Max/The Linkup Closes Its Doors,” http:// ww.techcrunch.com/2008/07/10/media max the linkup-closes its- doors/, July 2008.

[7] Amazon.com, “Amazon s3 Availability Event: July 20, 2008,” http://status.aws.amazon.com/s3-20080720.html, July 2008.

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007.

[10] M.A. Shah, R. Swaminathan, and M. Baker, “Privacy-Preserving Audit and Extraction of Digital Contents,” Cryptology ePrint Archive, Report 2008/186, 2008.

[11] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, “Deniable encryption,” in Crypto, 1997, pp. 90–104.

[12] A. Sahai and B. Waters. Fuzzy identity-based encryption. In EUROCRYPT, volume 3494, pages 457{473. Springer, 2005.

[13] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, EUROCRYPT, volume 6110 of Lecture Notes in Computer Science, pages 62{91. Springer, 2010.

[14] Benot Libert and Damien Vergnaud. Adaptive-id secure revocable identity-based encryption. In CT-RSA, pages 1{15, 2009.

[15] Tal Malkin, Daniele Micciancio, and Sara K. Miner. Efficient generic forward-secure signatures with an unbounded number of time periods. In Lars R. Knudsen, editor, EUROCRYPT, volume 2332 of Lecture Notes in Computer Science, pages 400{417. Springer, 2002.

[16] S. Micali. Efficient certificate revocation. LCS/TM 542b, Massachusetts Institute of Technology, 1996.

[17] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Tal Rabin, editor, CRYPTO, volume 6223 of Lecture Notes in Computer Science, pages 191{208. Springer, 2010.

[18] J. Qian and X. Dong. Fully secure revocable attribute-based encryption. Journal of Shanghai Jiaotong University (Science), 16(4):490{496, 2011.

Author’s Detail’s

Pappala Mohan Rao

Pursuing his M.Tech in the department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, AP, India. He obtained his B.Tech(IT) from ANITS in Vishakhapatanam.

Dr. Kasukurthi Venkata Rao

M.Tech, Ph.D working as Professor in the department of Computer Science and System Engineering, Andhra University College of Engineering, Visakhapatnam, A.P, India. His research field is in Image Processing, Web Technology, Quantum Cryptography, Data and Cyber Security.