Review Paper for Data Access Privilege Control with Fully-Anonymous ABE

Amol Dagu Shelkar1, Prof. Rucha Ravindra Galgali 2
Department of Computer and Science Engineering
Shreeyash College of Engineering, Aurangabad, Maharashtra, India

Abstract:
We propose a privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management. As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers. In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes.

Keywords: attribute based encryption, multi-authority, attribute based encryption.

I. INTRODUCTION
Cloud computing has been considered as a new model of enterprise IT infrastructure, which can organize huge resource of computing, storage and applications and enable users to enjoy ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources with great efficiency and minimal economic overhead. In a multi-authority ABE scheme, multiple attributeauthorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase [3] gave a multi-authority ABE scheme using the concepts of a trusted central authority(CA) and global identifiers (GID). For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group. Therefore, although the content of shared data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be re-signed by an existing user in the group. As a result, the integrity of the entire data can still be verified with the public keys of existing users only. Traditionally, this type of expressive access control is enforced by employing a trusted server to store data locally. The server is entrusted as a reference monitor that checks that a user presents proper certification before allowing him to access records or files. However, services are increasingly storing data in a distributed fashion across many servers. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the token and distributed erasure-coded data [8]. S. Kamara [9] described several architectures such as consumer architecture wishes to upload data, to verify the integrity of the data and to retrieve the data from the cloud. By invoking the data processor to upload the data, invoking the data verifier to verify the integrity of the data and invoking the token generator to retrieve the data that combine recent and non-standard cryptographic primitives in order to achieve the goal. The person who is trying to access the data is made to answer the security questions. A large amount of Decoy data is provided to the attacker which in turn protects the user's real data. The rest of the paper is organized as following: Section 2 provides an overview of the related work done in this area. It included algorithm, approach, and advantage. Section 3 gives system architecture of data access through cloud server with attribute authorities. Finally, conclusions are made along with future research.

II. RELATED STUDY
To protect stored data, it is not sufficient to use traditional network security techniques that are used for securing messages between pairs of users or between clients and servers. Sahai and Waters introduced attribute-based encryption (ABE) as a new means for encrypted access control. Public-Key encryption is a powerful mechanism for protecting the congeniality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device. In an attribute-based encryption system ciphertexts are not necessarily encrypted to one particular user as in traditional public key cryptography. Instead both users’ private keys and ciphertexts will be associated with a set of attributes or a policy over attributes.

I. (8) C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing”, 2012: Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast...
data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

II. (13) H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure threshold multi authority attribute based encryption without a central authority,”, 2010 : An attribute based encryption scheme (ABE) is a cryptographic primitive in which every user is identified by a set of attributes, and some function of these attributes is used to determine the ability to decrypt each ciphertext. Chase proposed the first multi authority ABE scheme in TCC 2007 as an answer to an open problem presented by Sahai and Waters in EUROCRYPT 2005. However, her scheme needs a fully trusted central authority which can decrypt every ciphertext in the system. This central authority would endanger the whole system if it’s corrupted. This paper presents a threshold multi authority fuzzy identity based encryption (MA-FIBE) scheme without a central authority for the first time. An encrypter can encrypt a message such that a user could only decrypt if he has at least of the given attributes about the message for at least2 honest authorities of all then attribute authorities in the proposed scheme. This paper considers a stronger adversary model in the sense that the corrupted authorities are allowed to distribute incorrect secret keys to the users. The security proof is based on the secrecy of the underlying joint random secret sharing protocol and joint zero secret sharing protocol and the standard decisional bilinear Hellman assumption. The proposed MA-FIBE could be extended to the threshold multi authority attribute based encryption (MA-ABE) scheme, and two secure MA-ABE schemes without a central authority are also presented in this paper. Moreover, some extensions about the proposed MA-ABE schemes, such as how to convert a large universe MA-ABE scheme into a proactive scheme, are also provided in this paper.

III. (17) V. Božović, D. Socek, R. Steinwandt, and V. I. Villányi, “Multi-authority attribute-based encryption with honest-but-curious central authority “, 2012: an attribute based encryption scheme capable of handling multiple authorities was recently proposed by chase. the scheme is built upon a single-authority attribute based encryption scheme presented earlier by sahai and waters. chase’s construction uses a trusted central authority that is inherently capable of decrypting arbitrary cipher text secured within the system. we present a multi-authority attribute based encryption scheme in which only the set of recipients defined by then encrypting party can decrypt a corresponding cipher text. the central authority is viewed as “honest-but-curious”: on the one hand it honestly follows the protocol, and on the other hand it is curious to decrypt arbitrary cipher texts thus violating the intent of the encrypting party. the proposed scheme, which like its predecessors relies on the bilinear diffie hellman assumption, has a complexity comparable to that of chase’s scheme. we prove that our scheme is secure in the selective id model and can tolerate an honest-but-curious central authority.

IV. (18) Nesrine Kaaniche, Maryline Laurent, "A Secure Client Side Deduplication Scheme in Cloud Storage Environments", 2014:

Recent years have witnessed the trend of leveraging cloud-based services for large scale content storage, processing, and distribution. Security and privacy are among top concerns for the public cloud environments. Towards these security challenges, we propose and implement, on OpenStack Swift, a new client-side deduplication scheme for securely storing and sharing outsourced data via the public cloud. The originality of our proposal is twofold. First, it ensures better confidentiality towards unauthorized users. That is, every client computes a per data key to encrypt the data that he intends to store in the cloud. As such, the data access is managed by the data owner. Second, by integrating access rights in metadata file, an authorized user can decipher an encrypted file only with his private key.

V. (19) Zhihua Xia, Xinhui Wang, Xingning Sun, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", 2015:

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF×IDF model are combined in the index construction and query generation. We construct a special tree-based index structure and propose a “Greedy Depth-first Search” algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.

III. PROPOSED WORK

In proposed work we proposed user revocation in users to enable activating and deactivating users. User Revocation is performed by the group manager. Delta Revocation List is publicly available based on those, group members are allowed to encrypt the data and make that data confident against revoked users. Revoked users are maintained in the revoke user list and make publicly available in the cloud. Delta RL is bounded by signature to declare its validity. Upon receiving the resignation request from the group member, group member will be in revoked user list. Group members are the registered users they will stockpile their private data into the cloud server and share the data among the group members. In our example, the employee plays the role of group members. It allows the group members to be dynamically changed, due to the staff resignation and the participation of new employee in the Organisation.
IV. SYSTEM DESIGN

![Diagram of cloud servers with sign in, user, and attributes]

V. PROPOSED WORK

We also address user revocation and our scheme prevents replay attacks. Multi-authority attribute-based encryption enables a more realistic deployment of attribute-based access control, such that different authorities are responsible for issuing different sets of attributes. Not only the access but also the operation should be controlled. Secondly, personal information (defined by each user’s attributes set) is at risk because one’s identity is authenticated based on his information for the purpose of access control. In future implemented model can be deployed on cloud and can be used by various companies. For implementation purpose we are considered the type of file as document file, text file which can be enhance to sound file, video file, image file etc. Also the set of attributes can be increased in order to provide high security to the model on cloud.

VI. REFERENCES


[6] Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization Brent Waters University of Texas at Austin bwaters@cs.utexas.edu


[14] CLOUD SECURITY USING FOG COMPUTING 1 S. RAJE, 2NAMRATA PATIL, 3 SHITAL MUNDHE, 4RITIKA MAHAJAN


