FULLY ANONYMOUS ATTRIBUTE BASED ENCRYPTION FOR PRIVILEGE AND ANONYMITY ACCESS CONTROL IN CLOUD


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 semianonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. 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.

I. INTRODUCTION

CLOUD Computing set up pervasive, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be immediately provision and released with essential efforts for management or service provider interaction. Its main objective is to deliver quick, secure, convenient data storage and net computing service, with all computing resources envision as services and delivered over the Internet.

A number of computing concepts and technologies are combined in Cloud Computing to satisfy the computing needs of users, it provides common business applications online through web browsers, while their data and software’s are stored on the servers. This is an approach that is used to maximize the scope or step up capabilities robustly without investing in new infrastructure, sustain new personnel or licensing new software. It provides tremendous storage for data and rapid computing to customers over the internet.

Data security is one of the aspects of the cloud which prohibit users from using cloud services. There is fear between the data owner’s especially in large organizations that their data possibly misuse by the cloud provider without their knowledge. Data security of the user’s can be ensured by using the concept of virtual private networks, firewalls, and by enforcing other security policies within its own circumferences.

Security is consequently an extensive element in any cloud computing environment, because it is crucial to assure that only authorized access is sanctioned and protected behaviour Is accepted.

Any kind of security and privacy contravention is critical and can produce crucial results. As soon as the strict regulations and policies are taken against privacy in cloud, more and more personnel will feel save to adopt cloud computing. A client may be individual or a big organization but all are having same concern i.e. data security, so data security is dire consequence. Data security at different levels is the vital matter of this technology; it can be categorized into two categories:

Security at External level and Security at Internal Level. Security at External level states that data is unsecure opposed to third party, cloud service provider or network intruder. Security at Internal level states that data is unsecure opposed to authorized users or employee of an organization.

A secure server plus provides a protected foundation for hosting your Web applications, and Web server configuration plays a critical role in your Web application’s security. Badly configured server can lead to unauthorized access. A forgotten...
share can provide a convenient back door, while an overlooked port can be an attacker's front door. Neglected user accounts can permit an attacker to slip by your defenses unnoticed. Understanding threats to your Web server and being able to identify appropriate countermeasures permits you to anticipate many attacks and thwart the ever growing numbers of attackers. This system provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication. In practice, this provides a reasonable guarantee that one is communicating with precisely. The website that one intended to communicate with, as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

Secure Server Plus application has mainly double login security. That is, after logging into the application user receives a secret key on his registered gmail id. This secret key has to be entered in the pop-up box displayed after logging into SSP Application. This application has two functionalities, Encryption and Decryption. Encryption is the functionality in which the file to be sent over mail in firstly divided into 4 equal parts in byte format and then encrypted using different encryption algorithms. After Encryption files would be sent to recipient through Gmail At the recipient end, He will download the files and using SSP Application data in files would be decrypted and merged.

II. RELATED WORKS

There are numerous work carried in the field of data protection at cloud. Many models, schemes and techniques are proposed for data security. M. Sugumaran et al [10] illustrates a couple of techniques that resolve the security of the data and proposes architecture to safeguard the data in cloud. In proposed architecture the encrypted data is stored in cloud using cryptography technique i.e. located on block cipher. Cindhamani.J et al [3] proposed an enhanced frame work for data security in cloud which follows the security policies such as integrity, confidentiality and availability. Parameters they used are 128 bit encryption, RSA algorithm and Trusted Party Auditor (TPA). Before storing the data into the cloud, the data owner assigns the privileges that who will access the data.

After assigning the privileges they encrypt the data and stores into the cloud. Dharmendra [4] proposed the unified data encryption architecture which ensures the data security and privacy with reasonable performance overhead of computing system. It is based on multilevel identity encryption approach with two level/factor identity verification process. Dr. L. Arockiam et al [5] achieves the data confidentiality in cloud storage with two different techniques i.e. encryption and obfuscation. Encryption encrypts the alpha-numeric and alpha data while obfuscation encrypts the numeric data. Both are done on user side. First, the user has to encrypt the data using any technique then he stores the data into cloud storage. Tae Hong et al [14] use two schemes to control the data privacy and the identity privacy. One is the AnonyControl scheme i.e. semianonymous privilege control scheme which not only addresses the data privacy but also the user identity privacy in extant access control schemes. It decentralizes the central authority to restrain the identity leakage and thus achieves semianonymity. Another is the AnonyControl-F scheme that controls the identity leakage and achieves the full anonymity. Eman M. Mohamed et al [6] Exhibits the data security model that is based on the analysis of cloud architecture and implemented software to intensify endeavor in data security model for cloud computing. Hu Shuijing [7] described the enormous essentials in cloud computing, such as security key technology, regulation and standard etc and discussed manner in which they are addressed.

In this Proposed model data is protected against all threats i.e. internal and external, thread during, transits as well as when data at rest.

III. PROPOSED WORK

The data confidentiality, less effort is paid to protect users’ identity privacy during those interactive protocols. Users’ identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes. We propose AnonyControl and AnonyControl-Fallow cloud servers to control users’ access privileges without knowing their identity information. In this setting, each authority knows only a part of any user’s attributes, which are not enough to figure out the user’s identity. The scheme proposed by Chase et al. considered the basic threshold-based KP-ABE. Many attribute based encryption schemes having multiple authorities have been proposed afterwards.

In our system, there are four types of entities: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers. A user can be a Data Owner and a Data Consumer simultaneously. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users’ personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

The proposed schemes are able to protect user’s privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F.

The proposed schemes are tolerant against authority compromise, and compromising of up to (N – 2) authorities does not bring the whole system down.
We provide detailed analysis on security and performance to show feasibility of the scheme AnonyControl and AnonyControl-F.

We firstly implement the real toolkit of a multi authority based encryption scheme AnonyControl and AnonyControl-F.

IV. LITERATURE SURVEY

1. Policy Attribute-Based Encryption With Privacy Preserving In Clouds

To decentralize Access Control Scheme for secure data storage (ABE & ABS). In this scheme we only give the privacy to attribute based encryption. And attribute based scheme. In attribute based encryption scheme we use the Anonym control Scheme.

2. Cipher text based policy attribute based encryption

As compared to existing schemes, our proposed solution enables the authority to revoke user attributes with minimal effort. We achieve this by uniquely integrating the technique of proxy re-encryption with CP-ABE, and enable the authority to delegate most of laborious tasks to proxy server.

3. Attribute Based data Shearing with attribute revocation

In this paper we focus on an important issue of attribute revocation which is cumbersome for CPABE schemes. In particular, we re-solve this challenging issue by considering more practical scenarios in which semi-trustable on-line proxy servers are available. As compared to existing schemes, our proposed solution enables the authority to revoke user attributes with minimal effort.

4. Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based

In existing system we only give the privacy to the data Access control, but not give the user identity privacy, in proposed system we give the privacy to the user identity. In this Scheme we use two scheme Anonym Control, and Anonym Control-F scheme. In this scheme we use the peer-to-peer protocol.

V. METHODOLOGIES

5.1 Registration Based Social Authentication Module

The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password), and then a few (e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice’s friend list and are appointed as Alice’s Registration.

5.2 Security Module

Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. Imagine a phishing email being sent from your mail because someone had forged your information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation. trustee-based social authentication systems ask users to select their own trustees without any constraint. In our experiments (i.e., Section VII), we show that the service provider can constrain trustee selections via imposing that no users are selected as trustees by too many other users, which can achieve better security guarantees.

5.3 Attribute based encryption

Attribute-based encryption module is using for each and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. the attribute-based encryption have been proposed to secure the cloud storage. Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter’s identity has some overlaps with the one specified in the ciphertext.

5.4 Multi-authority

A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above; guarantees the confidentiality of Data Consumers’ identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. This is the first implementation of a multi-authority attribute based encryption scheme.

VI. THE CLOUD SERVICE COMPOSITION MODEL

The Architecture encompasses bee agents and their interaction structure. i). Employee forager bee agent ii). Scout and onlooker bee agent. iii). Hive - Resource agent. There are a variety of users in the cloud platform. The cloud users must define their budgetary requirements based on technical and functional considerations.
VII. CONCLUSION

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users’ identity information. More importantly, our system can tolerate up to N – 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that AnonyControl both secure and efficient for cloud storage system.

The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalent secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes [39]–[41] who support efficient user revocation is one of our future works.

VIII. ACKNOWLEDGEMENTS

The authors offer their gratitude to their colleague Jingshan Yin, who implemented the 1-out-of-n protocol, and Shih-ming Huang from NCTU, who proofread their paper to correct minor errors.

REFERENCES


