Attribute-Based Data Sharing in Cloud Computing With Attribute Policy

Swarup kshatriya, Dr. Sandip M Chaware
Department of Computer Engineering
TSSM’s Bhivarabai Sawant College Of Engineering and Research, Narhe, Pune, India.
swarup.kshatriya@gmail.com
smchaware@gmail.com

Abstract—In recent adoption and diffusion of the facts and figures sharing paradigm in circulated systems such as online social systems or cloud computing, there have been increasing claims and anxieties for distributed facts and figures security. One of the most demanding matters in facts and figures sharing schemes is the enforcement of access principles and the support of principles updates. Cipher text policy attribute-based encryption (CP-ABE) is evolving an undertaking cryptographic solution to this issue. It endows facts and figures owners to characterize their own get access to principles over client attributes and enforce the policies on the facts and figures to be circulated. Although, the benefit arrives with a foremost drawback which is renowned as a key escrow difficulty. The key lifetime center could decrypt any notes addressed to specific users by developing their personal keys. This is not apt for facts and figures distributing scenarios where the facts and figures proprietor would like to make their personal facts and figures only accessible to designated users. In supplement, applying CP-ABE in the facts and figures sharing scheme inserts another dispute with regard to the client revocation since the get access to principles are characterized only over the ascribe universe. Thus, in this study, we suggest an innovative CP-ABE design for facts and by exploiting the figures sharing scheme at the attribute of the system architecture. Possibility of new designed suggested design features achieves two things, first is key escrow problem that could be explained by the escrow-free key generating another protocol, which is constructed utilizing the protected two-party computation between the key lifetime center and the data-storing center, and the second is fine-grained user revocation per each attribute could be finished by proxy encryption which takes advantage of the selective attribute assembly key circulation on top of the ABE.

The presentation and security analyses indicate that the suggested design is effective to securely organize the data distributed in the facts and figures distributing system. We proposed a encryption with efficient revocation scheme with central-control revocation, which is more suitable for large-scaled access control system. The improvement of secret key with binary tree structure can reduce the communication and computational costs in key update algorithm. Moreover, we demonstrated that the delegating capability can be easily provided in the proposed scheme, but all the delegates are restricted by their original delegators’ unique identifiers.

Index Terms— Attribute, CP-ABE, Data Sharing, Escrow Problem, Key Generation, Central-control revocation.

I. INTRODUCTION

Several circulated file and data schemes need complex access-control mechanisms, where get access to conclusions count upon attributes of the defended facts and figures and get access to policies allotted to users. Conventionally, such get access to-control means have been enforced by a server that acts as a trusted quotation monitor; the monitor will permit a client to view data only if it get access to principle permits it. While the use of trusted servers allows for a somewhat clear-cut answer, the raise a large downside to this approach both the servers and their storage should be trusted and stay uncompromised. With the increasing number of worm attacks and other forms of intrusion, sustaining the security of any specific owner is evolving progressively difficult. This problem is exacerbated in bigger schemes where sensitive facts and figures must be replicated over several servers because of scalability and survivability anxieties. A natural solution to this problem is to encrypt retained facts and figures in order to decrease data vulnerability in the event that a storage server is compromised. Although, traditional public-key encryption methods need that facts and figures be encrypted to one specific user’s public key and are unsuitable for expressing more convoluted get access to command policies. The concept of Attribute-Based Encryption (ABE). In Attribute-Based Encryption an encryption will associate encrypted data with a set of attributes. An authority will issue users different private keys, where a user’s private key is associated with an access structure over attributes and reflects the access policy ascribed to the user

Now days the use of cloud computing is increasing and end users making use of cloud services in order to save time and their resources. In data storage, the cloud allows the owner of data to store their personal and private information as well as share it with other peers using the cloud services only. The cloud services are either free or minimal fee-only applications
to cloud. It end-users can bring down cost efficiently. The command the user's access is to only authorize users for the purpose of the right to use the grating Efficient, secure, and scalable access control policy to use. [9]

Data sharing systems, data is uploaded to the server before encrypting the data privacy of data maintained by the data owner. Later we use only the data decryption keys that encrypted data is provided using shared system data such as methods of data. Security based on delivering the encryption and decryption methods, but there are many research challenges are introduced by such methods design. Cloud over data privacy is achieved by using encryption techniques. The security of network is consisting of different approaches and techniques to achieve the data cryptographic security. The most commonly used method in recent time is Attribute-based encryption (ABE).

Forward approach in which data cloud should be stored encrypted data before uploading to protect privacy are introduced traditional public key infrastructure data encryption process can be adopted, and the owner of cloud data prior to uploading the data to encrypt data uses the public key users; If a user sends through the access request to the cloud, the cloud will return to the same cipher text data user, a user to decrypt the data using your private key. But this manner would lead to some problems: (1) to be able to encrypt data, the data owner needs to obtain the data user's public key to complete this; (2) a lot of storage overhead would spend because of the same plaintext with different public keys. In order to overcome these limitations, and so forth, an attribute-based encryption (ABE) Scheme [5] proposed in 2005, and attribute-based encryption scheme first proposed this concept paper identifying a user properties. ABE as a set of attributes, used to encrypt and to decrypt data that was used for ABE can result that, the data plan issue owner didn't want to share data from memberships. A non-negative attribute to exclude the parties with whom data access policy controls in data sharing systems. In this section we are presenting the different methods security at data sharing systems. In section III, the proposed approach and its system block diagram is depicted. In section IV we are presenting the current state of implementation and results achieved. Finally conclusion and future work is predicted in section V.

II. LITERATURE SURVEY

In this section we are presenting the different methods those are presented to solve the trust problems security and access policy controls in data sharing systems. A. Boldyreva, V Goyal, Kumar V any PKI or identity-based, system settings, users must provide a means to cancellation so efficient traditional PKI settings a. well studied problem. However, in the setting of the revocation Mechanism of IBE studies on most demand. Arik solutions also require senders to use time periods when encrypting, and all receiver (regardless whether their keys have been compromised) by contacting their respective keys trusted authority regularly updated. It has been noted that this solution, as well as the number of growth-scale, becomes a bottleneck work on important updates. He enhances key update efficiency (linear logarithmic in the number of users), on the edge of a trusted party proposes plans IBE, while users remain efficient. our plan fuzzy IBE primitive and binary tree data structure builds on the ideas of, And provably secure.

N. Attrapadung and H. Imai they presents Attribute-based encryption (ABE) system enables an access control mechanism over encrypted data by specifying access policies among private keys and cipher texts. There are two flavors of ABE, namely key-policy and cipher text-policy, depending on which of private keys or cipher texts that access policies are associated with. In this paper they propose a new cryptosystem called Broadcast ABE for both flavors. Broadcast ABE is used to construct and generate the ABE systems by using direct revocation mechanism process. Direct revocation has useful characteristics and all properties of revocation that can be done without affecting on non-revoked users; in particular, which does not require users to update keys periodically. For key-policy variant, our

In [13], Muller ET proposed a distributed attribute-based encryption scheme; Yu et al. [14] proposed a fine-grained data access control encryption scheme , Tang et al. [15] proposed a certificate qualified attribute-based encryption scheme, and Wang [16] proposed A hierarchical attribute-based encryption scheme (HABE) proposed in 2010 and 2011. This plan uses generic form voyage policy and key generates a hierarchically. And this scheme assumed that all attributes in one conjunctive clause are administered by the same domain authority. In addition to this, there are multi authorities ABE schemes [17] [18] that use multiple parties to distribute attributes for users Presented very recently [1] new safe and effective method that feature-based method of data sharing system [1] by exploiting a fine-grained data access control to implement shared data. Practically the better efficiency, scalability and security, overcoming the limitations of existing methods show the method of its credibility as it handles many requests to single-user key generators System uses therefore this paper we in detail to achieve the goal with this method, are aiming to improve the security, reliability, load balancing and therefore efficiency. In next section II we are presenting the literature survey over the various methods security at data sharing systems. In section III, the proposed approach and its system block diagram is depicted. In section IV we are presenting the current state of implementation and results achieved. Finally conclusion and future work is predicted in section V.
systems should appear to be the first fully functional and directly revocable schemes. For cipher text-policy variant, proposed system improves the efficiency from the previously best revocable schemes; in particular, one of our schemes admits a cipher text and sizes of private key roughly the same as the already available non-revocable cipher text-policy ABE. Broadcast ABE also that can be utilized to construct multi-authority ABE in the disjunctive setting.

M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. They have done Attributes define, classify, or annotate the datum to which they are assigned. However, traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments. In this paper, they introduce a novel secure information management architecture based on existing attribute based encryption (ABE) primitives. A policy system that meets the needs of complex policies is defined and illustrated. Based on the needs of those policies, they propose cryptographic optimizations that vastly improve enforcement efficiency. They further explore the use of such policies in two example applications: a HIPAA compliant distributed file system and a social network. A performance analysis of our ABE system and example applications demonstrates the ability to reduce cryptographic costs by as much as 98% over previously proposed constructions. Through this, they demonstrate that their attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems.

S. Yu, C. Wang, K. Ren, and W. Lou. They represent a Cipher text-Policy Attribute Based Encryption (CP-ABE) is a promising cryptographic primitive for fine-grained access control of shared data. In CP-ABE, each user is associated with a set of attributes and data are encrypted with access structures on attributes. A user is able to decrypt a cipher text if and only if his attributes satisfy the cipher text access structure. Besides this basic property, practical applications usually have other requirements. In this paper they focus on an important issue of attribute revocation which is cumbersome for CP-ABE schemes. In particular, they resolve 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. They 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 servers. Formal analysis shows that our proposed scheme is provably secure against chosen cipher text attacks. In addition, they show that our technique can also be applicable to the Key-Policy Attribute Based Encryption (KP-ABE) counterpart.

D. Boneh and M.K. Franklin, They propose a fully functional identity-based encryption scheme (IBE). The scheme has chosen cipher text security in the random oracle model assuming a variant of the computational Die Hellman problem. Their system is based on linear maps between groups. The Weil pairing on elliptic curves is an example of such a map. They give precise definitions for secure identity based encryption schemes and give several applications for such systems.

L. Cheung and C. Newport, in cipher text policy attribute-based encryption (CP-ABE), every secret key is associated with a set of attributes, and every cipher text is associated with an access structure on attributes. Decryption is enabled if and only if the user's attribute set satisfies the cipher text access structure. This provides fine-grained access control on shared data in many practical settings, including secure databases and secure multicast. In this paper, they study CP-ABE schemes in which access structures are and gates on positive and negative attributes. Our basic scheme is proven to be chosen plaintext (CPA) secure under the decisional bilinear Daffier-Hellman (DBDH) assumption. Then they have applied the Canetti-Halevi-Katz technique to obtain a chosen cipher text (CCA) secure extension using one-time signatures. The security proof is a reduction to the DBDH assumption and the strong existential unforgeability of the signature primitive. In addition, they introduce hierarchical attributes to optimize our basic scheme—reducing both cipher text size and encryption/decryption time while maintaining CPA security. Finally, we propose an extension in which access policies are arbitrary threshold trees, and we conclude with a discussion of practical applications of CP-ABE.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

3.1 Problem Definition

This paper presented the way for secure data sharing for cloud computing. This paper giving the approach which is presented for improving the security and efficiency in attribute-based data sharing. This method significantly overcomes the drawbacks of all previous methods such as key escrow problem and scalability, processing speed as well as backup problem and data storing traffic problem.

The literature review presented many methods for secure data sharing in cloud computing. However in the system there are some disadvantages that got identified, we need to improve secret key with binary tree structure can reduce the communication and computational costs in key update algorithm.

3.2 Proposed Architecture and Design

In the proposed paper, Revocation is the vital component in CPABE, that must be designed and generate into the system from the starting rather than being added after getting the other issues are addressed, it is necessary to give careful planning on where functionality must be placed and how to reduce the communication costs and computational. The paradigm of revocation would be categorized into two designs called as central-control and another one is user-control. In a central-control design, system manager or a trusted third parties T centrally maintains revocation lists. Encrypters runs encryption algorithms without being aware of those revocation lists, while descriptors that need to keep updating their secret keys as it is with additional update information dataset periodically generated by T, which would cost more for decryption process.
At the user-control design, system manager is only involved in the initialization phase while revocation scheme is implemented in encryption algorithms by encrypters.

A Key update algorithm is designed and added for respectively enabling and disabling the decryption, ability of non-revoked users and revoked users. Encryption algorithm has an extra encryption time \( t \), that indicating the output cipher text can be only decrypted by non-revoked users at time \( t \). Decryption algorithm has an additional input, update information \( UI \), only assisting no revoked users’ decryption.

3.3 Algorithm

A Revocable Cipher text Policy Attribute Base Encryption process includes a tuple of Probabilistic Polynomial-Time (PPT) Algorithms.

1. Set up \((U, n_{max})\) the setup algorithm takes the universal attribute set \( U \) and the maximum Index is \( n_{max} \) of columns in an access structure as inputs. It outputs the public parameters \( PP \) and a master key \( MK \).
2. KGen \((uid, S, MK)\) the key generation algorithm takes a unique identifier is \( uid \), an attribute Set is \( S \subseteq U \) and the master key is \( MK \) as inputs. It outputs a secret key \((uid, SK)\) to the user.
3. KUpd \((rl, t, MK)\) The key update algorithm takes a revocation list is \( rl \), a time stamp denoted as \( t \) and the master key as \( MK \) as inputs. It outputs the update information is \( UI \).
4. Enc \((PP, (M, \rho), M, t)\) the encryption algorithm takes the public parameters \( PP \), an access structure \((M, \rho)\), a message \( M \) and a time stamp \( t \) as inputs. It outputs the cipher text \( C \) with \((M, \rho)\).
5. Dec\((C, (M, \rho), SK, UI)\) the decryption algorithm takes the cipher text \( C \) with \((M, \rho)\), the secret key \( SK \) and the update information \( UI \). If the attribute set related with \( SK \) satisfies the access structure \((M, \rho)\) and the unique identifier associated with \( SK \) has not been revoked in update information \( UI \), it decrypts the ciphertext and returns a message \( M \);
6. else, it returns.

IV. REQUIREMENT SPECIFICATION

In this section we are representing the input and practical environment.

4.1 Input

Different files for the purpose of upload and download. And also username and password are input for login.

4.2 Hardware and Software Requirement

Hardware Configuration
- Processor - Pentium –IV
- Speed - 1.1 GHz
- RAM - 256 MB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard.
- Monitor – SVGA

Software Configuration
- Operating System: Window XP/7/8
- Programming language: JAVA
- Database: SQL-YOG
- Tools: Net Beans

V. CONCLUSION AND FUTURE WORK

Now days, the access policies enforcement and support of policy update are one of the huge challenging problems in a research mechanism of data sharing systems. In this proposed
paper we have presented the new system which based on efficient security method which recently presented. The existing scheme was totally based on attribute based data sharing security. In this proposed method Revocable Cipher text Policy Attribute Based Encryption scheme with central-control revocation, which is more suitable for large-scaled access control system. The improvement of secret key with binary tree structure can reduce the communication and computational costs in key update algorithm. Moreover, we demonstrated that the delegating capability can be easily provided in the proposed scheme, but all the delegates are restricted by their original delegates’ unique identifiers. For our future work, the efficiency of Revocable Cipher text Policy Attribute Based Encryption schemes will be improved, such as shortening the size of secret key, reducing the amount of update information, and developing faster encryption/decryption algorithms.

REFERENCES


