PRIVACY-PRESERVING APPROACH TO POLICY-BASED CONTENT DISSEMINATION USING KEY-MANAGEMENT

#1 MURAHARI SURESH, M.Tech Student,
#2 P.ESWARAIAH, Assistant Professor, 
Department Of CSE, 
BVSR ENGINEERING COLLEGE,CHIMAKURTHY, PRAKASAM, A.P, INDIA.

Abstract: Cloud computing is revolutionizing many ecosystems by providing organizations with computing resources featuring easy deployment, connectivity, configuration, automation and scalability. This paradigm shift raises a broad range of security and privacy issues that must be taken into consideration. Multi-tenancy, loss of control, and trust are key challenges in cloud computing environments. This paper reviews the existing technologies and a wide array of both earlier and state-of-the-art projects on cloud security and privacy. In this paper, we propose CloudKeyBank, the first unified key management framework that addresses all the three goals above. Under our framework, the key owner can perform privacy and controllable authorization enforced encryption with minimum information leakage. To implement CloudKeyBank efficiently, we propose a new cryptographic primitive named Searchable Conditional Proxy Re-Encryption (SC-PRE) which combines the techniques of Hidden Vector Encryption (HVE) and Proxy Re-Encryption (PRE) seamlessly, and propose a concrete SC-PRE scheme based on existing HVE and PRE schemes. Our experimental results and security analysis show the efficiency and security goals are well achieved.

Keywords: SC-PRE, Search Privacy, Key Management, Keys Outsourcing.

I. INTRODUCTION

Cloud storage means “the storage of data online in the cloud,” where the data is put away in and available from different distributed and connected resources that compromise a cloud. However, the cloud storage is not completely trusted. Whether the data put away on cloud are in place or not turns into a significant concern of the clients. So to secure data and client Identity; Identity Based Encryption (IBE) is an interesting option, which is proposed to streamline key administration in an authentication, based on Public Key Infrastructure (PKI) by utilizing humancoherent Identities (e.g., remarkable name, email address, IP address, and so forth) as open keys. Along these lines, sender utilizing IBE does not have to gaze upward open key and authentication, however specifically scrambles message with recipient’s Identities. As needs be, beneficiary getting the private key related with the comparing Identity from Private Key Generator (PKG) can decrypt such cipher text. In Boneh and Franklin recommended that clients update their private keys intermittently and senders utilize the beneficiaries’ Identities connected with current time period. In any case, this mechanism would bring about an overhead load at PKG. In another word, every one of the clients paying little respect to whether their keys have been revoked or not, need to contact with PKG intermittently to demonstrate their Identities and redesign new private keys. It requires that PKG is online and the safe channel must be kept up for all exchanges, which will end up being a bottleneck for IBE framework as the quantity of clients develops of systems. In this paper, we bring outsourcing computation into IBE revocation, and formalize the security meaning of outsourced revocable IBE interestingly to the best of our knowledge.

II. LITERATURE SURVEY

The accessibility of quick and dependable Digital Identities is a key element for the fruitful execution of the general population key base of the Internet. All computerized character plans must incorporate a technique for denying somebody's advanced character for the situation that this character is stolen (or wiped out) before its termination date (like the cancelation of a Master cards for the situation that they are stolen). In 1995, S. Micali proposed a rich strategy for personality denial which requires almost no correspondence in the middle of clients and varies in the framework. In this paper, we expand his plan by decreasing the general CA to Directory correspondence, while as yet keeping up the same minor client to seller correspondence. We differentiate our plan to different recommendations also. In this paper the author Consider a powerless customer that wishes to delegate calculation to an untrusted server and have the capacity to briefly confirm the accuracy of the outcome. We display conventions in two loose variations of this issue. We rst consider a model where the customer delegates the calculation to two or more servers, and is ensured to yield the right reply for whatever length of time that even a solitary server is straightforward. In this model, we demonstrate a 1-round measurably solid convention for any log-space uniform NC circuit. Interestingly, in the single server setting all known one-round concise designation conventions are computationally solid. The convention develops the arithmetiation systems of [Goldwasser-Kalai-
Rothblum, STOC 08] and [Feige-Kilian, STOC 97]. Next we consider a implied perspective of the convention of [Goldwasser-Kalai-Rothblum, STOC 08] in the single-server model with a nonconcise, however open, one stage. Utilizing this simplification we build two computationally stable conventions for appointment of calculation of any circuit C with profundity d and data length n, even a non-uniform one, such that the customer keeps running in time n poly(log(JC)); d). The rst convention is conceivably down to earth and less demanding to actualize for general calculations than the full convention of [Goldwasser-Kalai-Rothblum, STOC 08], and the second is a 1-round convention with comparative many-sided quality, yet less client server. In this paper [5] the author addresses the issue of utilizing untrusted (possibly malevolent) cryptographic partners. We give a formal security definition to safely outsourcing calculations from a computationally constrained gadget to an untrusted partner. In our model, the ill-disposed environment composes the product for the partner, however then does not have direct correspondence with it once the gadget begins depending on it. Notwithstanding security, we likewise give a structure to measuring the effectiveness also; check ability of an outsourcing usage. We introduce two pragmatic outsource secure plans. In particular, we demonstrate to safely outsource measured exponentiation, which presents the computational bottleneck in most open key cryptography on computationally restricted gadgets. Without outsourcing, a gadget would require O (n) particular augmentations to complete particular exponentiation for n-bit types. The heap lessens to O(log2 n) for any exponentiation-based plan where the genuine gadget may utilize two untrusted exponentiation programs; we highlight the Cramer-Shoup cryptosystem and Schnorr marks as samples. With a casual thought of security, we accomplish the same burden diminishment for another CCA2-secure encryption plan utilizing stand out untrusted Cramer-Shoup encryption program. In this paper [6] the author demonstrated that the Trait based encryption (ABE) is a promising cryptographic apparatus for fine-grained access control. Be that as it may, the computational taken a toll in encryption ordinarily develops with the many-sided quality of access arrangement in existing ABE plans, which turns into a bottleneck constraining its application. In this paper, we formulize the novel worldview of outsourcing encryption of ABE to cloud administration supplier to calm neighbourhood calculation trouble. We propose an enhanced development with Map Reduce cloud which is secure under the suspicion that the expert hub and in addition at minimum one of the slave hubs is straightforward. In the wake of outsourcing, the computational taken a toll at client side amid encryption is decreased to inexact four exponentiations, which is steady. Another point of preference of the proposed development is that the client can assign encryption for any arrangement. In this paper [7] the author studied that the vast scale picture information sets are as a rule exponentially created today. Alongside such information blast is the quickly developing pattern to outsource the picture administration frameworks to the cloud for its rich processing assets and benefits. How-to ensure the delicate information while empowering outsourced picture administrations, be that as it may, turns into a noteworthy concern. To address these difficulties, we propose outsourced picture recuperation administration (OIRS), a novel outsourced picture recuperation administration construction modelling, which abuses diverse area advances and takes security, efficiency, and outline many-sided quality into thought from the earliest starting point of the administration. Specifically, we plan OIRS under the compacted detecting system, which is known for its effortlessness of binding together the conventional examining and pressure for picture securing. Information proprietors just need to outsource packed picture tests to cloud for lessened stockpiling overhead. What's more, in OIRS, information clients can tackle the cloud to safely reproduce pictures without uncovering data from either the compacted picture tests or the fundamental picture content. We begin with the OIRS plan for scanty information, which is the ordinary application situation for packed detecting, and after that demonstrate its common expansion to The general information for important trade-offs in the middle of efficiency and exactness. We altogether break down the security assurance of OIRS and behavior broad examinations to exhibit the framework viability and efficiency. For fulfillment, we additionally examine the normal execution speedup of OIRS through equipment assembled in framework outline. Framework viability and efficiency. For fulfillment, we additionally examine the normal execution speedup of OIRS through equipment assembled in framework outline.

III. SYSTEM ARCHITECTURE AND ATTACK SURFACE

In this section we first describe the CloudKeyBank system architecture, and then based on which we give the attack surface.

A. CloudKeyBank System Architecture

As shown in Fig.3, CloudKeyBank architecture consists of four entities: Key owner, CloudKeyBank provider, Trusted client and Users.

1) Key owner. Key owner can be the password owner or data encryption key owner who outsources his/her encrypted key database (Key DB) to the CloudKeyBank provider. After that the encrypted key database (EDB) stored in CloudKey- Bank provider can be accessed anywhere and anytime with minimum information leakage such as the size of Key DB. The key owner mainly completes the following three tasks:
1) Constructing the customized access control policy (ACP) in terms of his/her practical keys sharing requirements;
2) Depositing Key DB by using DepositKey protocol under the support of ACP;
3) Distributing authorized Query tokens to the delegated user based on the user’s registered information such as the wanted query and physical identity.

2) CloudKeyBank provider. CloudKeyBank provider can be any professional password manager such as LastPass who provides privacy enforced access control on EDB. The Cloud- KeyBank provider mainly completes the following two tasks:
1) To enforce the privacy of identity attributes in the Search attribute group, he/she can perform search query directly by evaluating the submitted Query token against the encrypted key tuples in EDB;
2) To enforce the key authorization he/she can transform an encrypted key into the authorized re-encrypted key under the corresponding Delegation token stored in Authorization Table (AuT).

![Fig. 1. CloudKeyBank System Architecture](image)

3) Trusted client. Trusted client is the primary privacy enforced component in CloudKeyBank framework. It mainly consists of two protocols: DepositKey and WithdrawKey.

4) Users. There are two kinds of users in CloudKeyBank framework: Key owner and Collaboration group. Key owner corresponds to an individual user who deposits all his keys to CloudKeyBank provider and access them by himself. Collaboration group corresponds to a group of users where the key owner can share his/her keys with other users within the same collaboration group. By submitting the private key and authorized Query token, a delegated user can withdraw an authorized key by using WithdrawKey protocol under the support of privacy enforced access control policy (i.e. AuT in our solution).

As is shown in Fig. 1, Service providers, such as web based application providers and outsourced data storage providers, are the part in the dotted cloud. In this paper we assume the secure communication (protecting the security of transferred name and key) between users and service providers is based on HTTPS and outsourced data stored at these service providers are encrypted under data encryption keys. In this paper we only focus on how to achieve the privacy and owner controllable authorization of keys stored in CloudKeyBank provider, while do not consider the privacy of outsourced data protected by the keys.

B. Attack Surface

In CloudKeyBank architecture, based on outsourced key tuple ti = f-xi; ~kig, we focus on the attacks on sensitive key attributes ~ki and sensitive identity attributes ~xi. Corresponding to the attacks there mainly exist the following three kinds of attackers:
1) Attacker1: CloudKeyBank provider is a honest-but-curious inside attacker who is curious about key values in ~ki (Key confidentiality) and identity values in ~xi (Identity confidentiality and Linkability privacy), but can honestly provide efficient database operations given minimum information leakage. The minimum information leakage may include leakage on the total size of the Key DB and on random tuple identifier (e.g. the identifier indi for tuple to speed up the query efficiency), but never the direct exposure of plaintext keys or identities;
2) Attacker2: The malicious user is an outside attacker who wants to derive keys of the delegated user and thus impersonate him/her to do illegal actions (Key privacy and Key authorization);
3) Attacker3: The CloudKeyBank provider or the attacker in the middle may derive the private intent of the user from his/her submitted search query (Search privacy);
4) Attacker4: The malicious user may impersonate the legal user to submit search query in terms of the known background knowledge such as the possible search keywords (Query authorization).

IV. IMPLEMENTATION METHODOLOGY

In recent years academia and industry have paid more attention to privacy problems in outsourcing scenario. In the following sections, we just describe the related work based on which our solution is developed.

A. Encryption based privacy and authorization in DaaS

Hacigumus et al [13] first introduced the concept of Database as a Service (DaaS) for outsourced database management. To guarantee privacy and access authorization of outsourced data, data owners employ different cryptographic techniques to encrypt data so as to implement different goals of privacy protection. For example bucketization encryption [14], order preserving encryption [23] and B+ based encryption [21] were proposed to support efficient queries on encrypted data with less privacy...
leakage. The approaches in [13] mainly guarantees the confidentiality and privacy of data by encrypting data tuples in an all or nothing way. Policy based encryption [18][22][24][25][26] were proposed to encrypt data in such a way that only users who were permitted to access data in terms of the access policies could be able to do so. Therefore efficient key management determined by the access control policy becomes the primary factor of policy based encryption. The approaches in [18][26] focuses on achieving the identity and authorization privacy of users by encrypting identity attributes and related identity based conditions in the access control policy. Bertino et al [20] proposed an unified framework for an outsourced medical database to enforce the privacy and copyright protection by combining techniques of binning and digital watermarking. However, to the best of our knowledge, there is no related research on how to provide the privacy and owner authorization enforced key management for large number of web based applications and outsourced data storage. We tackle the problem in this paper.

B. Conjunctive keywords and search on encrypted data

Searchable encryption consists of searchable symmetric encryption (SSE) introduced by Song et al[2] and public encryption with keyword search(PKES) introduced by Boneh et al[3]. Based on SSE, the approaches proposed in [15][16] mainly achieves the conjunctive search privacy on data tuples of scalable encrypted database. Based on PKES, the concept of predicate encryption [3][4], allowing searches on encrypted data without a private key that corresponds to a public key, was created. In predicate encryption scheme, a service provider is given a token, instead of the full private key, for evaluating one or more predicates on the encrypted data[7]. Hidden vector encryption(HVE) [6] is one kind of predicate encryption where two vectors over attributes are associated with a ciphertext and a token respectively. HVE supports conjunctive search queries over encrypted data. HVE schemes proposed in[6][5][7] are constructed on bilinear groups with a composite order. Katz [12] extended the predicate encryption to support disjunction and inner product. But due to the high cost of computation on exponentiation and bilinear pairings, Katz [8] proposed a scheme based on prime group which requires a token size of $O(n)$ and $O(n)$ pairing computation, when n is the number of attribute conjunctions. It still results in the huge query cost because each of the ciphertexts could be a valid ciphertext that matches the token. Park proposed a low cost HVE [10][11] scheme which is also based on pairing group but only requires a $O(1)$ token size and $O(1)$ pairing computation. Therefore following predicate privacy in [9] and scheme proposed in Park [10][11], based on search attribute group $\sim xi$ of key tuple $ti$ we introduce two vectors to guarantee the search privacy on conjunctive identity attributes.

C. Proxy re-encryption with keyword search

In 1998, Blaze et al [18] introduced a concept of proxy re-encryption(PRE) where a proxy can re-encrypt a ciphertext from the sender to a re-ciphertext decrypted under the private key of the receiver. There are two types of PRE, one is based on the re-encryption direction including bidirectional and unidirectional, the other is based on the number of hops including single hop and multi-hop. In 2005 Atieniese et al [19] presented different unidirectional schemes using bilinear maps and showed how to prevent proxies from colluding with delegates to derive the delegator’s secret key. From then on, Many different type of PRE schemes are proposed. Proxy re-encryption with keyword search (PRES) introduced by Shao et al enables a proxy to transfer the re-ciphertext to a delegatee in a way that the keyword search can be performed on the ciphertext by using a keyword token. PRES scheme proposed in can guarantee the privacy of keyword. Conditional proxy re-encryption (C-PRE) introduced by Weng et al provided a solution to enforce the conditional delegation capabilities of the delegator where only ciphertexts satisfying a certain keyword condition set by the delegator can be transferred by the proxy. To further enforce keyword privacy and fine-grained conditional delegation capability of the delegator, Fang et al. introduced anonymous PRE and hierarchical proxy re-encryption (H-PRE) respectively. HPRE extends the single keyword based delegation to conjunctive keywords based delegation. However, to date, the major work proposed has focused on single keyword search and no proposed C-PRE schemes can support hidden multi keyword based search on ciphertext.

V. CONCLUSION

Focusing on issue of identity revocation, we have introduced outsourcing computation into IBE and proposed a revocable scheme in which the revocation operations are delegated to CSP. To solve the identified critical security requirements for keys outsourcing, we present CloudKeyBank, the first unified privacy and owner authorization enforced key management framework. To implement CloudKeyBank, we propose a new cryptographic primitive SC-PRE and the corresponding concrete SC-PRE scheme. The security comparison and analysis prove that our solution is sufficient to support the identified three security requirements which are not be solve in traditional outsourced scenario. From the performance analysis, we can see that our solution is not so efficient because it requires several seconds to answer a query on a database only 200 passwords. The main reason for inefficiency is that SC-PRE belongs to one kind of public encryption which is inefficient in common by comparing to the symmetric encryption. That
is what we want to solve in our future work where we will introduce searchable symmetric encryption, bloom filter based index in one server, and access policy enforcement in another server to support scalable operations on encrypted key database.

REFERENCES


of access control evolution on outsourced data. *Proc of 29th International Conference on Very Large Data Bases (VLDB '07)*, pages 123-134, 2007.


