International Journal of Engineering In Advanced Research Science and Technology
ISSN: 2278-2566
VOLUME-2
ISSUE-5
NOV-2016

PRIVACY AND OWNER AUTHORIZATION SYMMETRIC ENCRYPTION, WITH BLOOM FILTER

p.suri babu [1],v.sudhakar[2]
[1]M.Tech Student, Dept.Of CSE, Sarojini Institute of Technology, Telaprolu(V), Unguturu (M), Gannavaram, krishna (D). A.P
[2]Assistant Professor, Dept.Of CSE, Sarojini Institute of Technology, Telaprolu(V), Unguturu (M), Gannavaram, krishna (D). A.P

ABSTRACT:

Explosive growth in the number of passwords for web based applications and encryption keys for outsourced data storage well exceed the management limit of users. Therefore outsourcing keys (including passwords and data encryption keys)to professional password managers (honest-but-curious service providers) is attracting the attention of many users. However, existing solutions in traditional data outsourcing scenario are unable to simultaneously meet the following three security requirements for keys outsourcing: 1)Confidentiality and privacy of keys; 2)Search privacy on identity attributes tied to keys 3)Owner controllable authorization over his/her shared keys. In this paper, we propose Cloud Key Bank, 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 Cloud Key Bank 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 SCPRE scheme based on existing HVE and PRE schemes. With Bloom Filter.

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

INTRODUCTION :

From the perspective of service delivery, NIST has analyze three basic types of cloud service contribution. These models are: (i) Software as a service (SaaS) which offers lease application functionality from a service provider rather than buying, installing and running software by the user. (ii) Platform as a service (PaaS) which provides a platform in the cloud, beginning with which applications can be developed and completed. (iii) Infrastructure as a service (IaaS) in which the vendors offer computing power and storage space on appeal. From a hardware point of view, three attitude are new in the paradigm of cloud computing (Armbrust et al., 2009). These attitude of cloud computing are: (i) The illusion of absolute computing resources accessible on demand, thereby eliminating the need for cloud computing users to plan far ahead for provisioning. (ii) The expulsion of an up-front commitment by cloud users, thereby grant companies to start small and increase hardware assets only when there is an increase in their needs. (iii) The capability to pay for use of computing resources on a short-term basis as needed and release them when the assets are not needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful. In a nutshell, cloud computing has facilitate operations of large-

scale data centers which has led to compelling decrease in operational costs of those data centers. On the consumer side, there are some accessible benefits provided by cloud computing. A painful existence of running IT services is the fact that in most of the times, peak appeal is significantly higher than the average appeal. The resultant enormous over-provisioning that the companies usually do is acutely capital-intensive and wasteful. Cloud computing has grant and will allow even more seamless scaling of assets as the demand changes. In spite of the distinct advantages that cloud computing brings along with it, there are distinct concerns and issues which need to be solved before ubiquitous approval of this computing paradigm happens. First, in cloud computing, the user may not have the kind of control over his/her data or the conduct of his/her applications that he/she may need, or the capability to audit or change the processes and policies beneath which he/she must work. Different parts of an application might be in disparate place in the cloud that can have an conflicting impact on the performance of the application. Complying with adjustment may be difficult exclusively when talking about cross-border issues – it should also be noted that adjustment still need to be advanced to take all aspects of cloud computing into account. It is absolutely natural that monitoring and maintenance is not as simple a task as correlated to what it is for PCs sitting in the Intranet. Second, the cloud customers may risk losing data by having them locked into antidote formats and may lose control over their data since the tools for monitoring who is using them or who can aspect them are not always administer to the customers. Data loss is, therefore, a probably real risk in some specific deployments. Third, it may not be easy to tailor service-level agreements (SLAs) to the definite needs of a business. Compensation for downtime may be deficient and SLAs are unlikely to cover the concomitant damages. It is astute to balance the cost of guaranteeing domestic uptime against the advantages of decide for the cloud. Fourth, leveraging cost advantages may not always be achievable always. From the aspect of the organizations, having little or no capital expenditure may indeed have tax disadvantages. Finally, the measure are immature and deficient for handling the rapidly changing and evolving technologies of cloud computing. Therefore, one cannot just move applications to the cloud and forecast them to run efficiently. Finally, there are inactivity and performance argument since the Internet connections and the network links may add to inactivity or may put constraint on the available bandwidth.

The rapid deployment of web applications such as online banking, shopping, social networks and data storage (e.g., Amazon S3 and Google Drive), advising the ever-growing number of passwords and data encryption keys is becoming a big burden for abounding users. To remember them, 85% students admit that their passwords are essentially the same barring for bank and email accounts. However, the weak and common passwords

across accounts make them easy to be negotiate, which in turn leaks more passwords associated to private and delicate data. The success of web based password controller such as Last pass(1), with over a million users in 2011, Password Box(2), with over a million users in less than three months in 2013, and other analogous tools(345), demonstrate that users have a strong will to outsource their passwords to a centralized key management provider who can alleviate them from the overwhelming burden of memorization and authority.

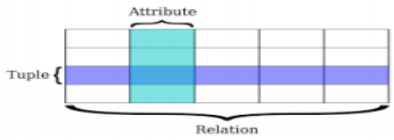
As per the explanation provided by the National Institute for Standards and Technology (NIST) (Badger et al., 2011), "cloud computing is a model for permissive convenient, on-demand network approach to a common pool of configurable computing assets (e.g., networks, servers, cache, applications, and services) that can be briskly provisioned and released with essential management effort or assistance provider interaction". It perform a paradigm shift in advice technology many of us are likely to see in our lifetime. While the customers are agitated by the opportunities to curtail the capital costs, and the chance to deprive themselves of infrastructure management and focal point on core competencies, and above all the dexterity offered by the on-demand apparatus of computing, there are argument and challenges which need to be forward before a ubiquitous approval may happen. Cloud computing assign to both the applications conveyed as services over the Internet and the plumbing and systems software in the data centers that arrange those services. There are four elemental cloud delivery models, as outlined by NIST (Badger et al., 2011), based on who arrange the cloud services. The company may employ one model or a merger of different models for adequate and optimized distribution of applications and business assistance. These four distribution models are: (i) Private cloud in which cloud assistance are arrange solely for an organization and are educated by the organization or a third party. These assistance may exist off-site. (ii) Public cloud in which cloud assistance are available to the public and purchased by an organization selling the cloud assistance, for example, Amazon cloud assistance. (iii) Community cloud in which cloud services are shared by definite organizations for auxiliary a specific community that has common concerns (e.g., mission, security requirements, policy, and conformity considerations). These assistance may be managed by the organizations or a third party and may continue offsite. A special case of association cloud is the Government or G-Cloud. This type of cloud computing is afford by one or more company(service provider role), for use by all, or most, government company (user role). (iv) Hybrid cloud which is a architecture of different cloud computing base (public, private or community). An example for hybrid cloud is the data stored in exclusive cloud of a travel department that is manipulated by a program running in the popular cloud.

1.2 Key Encryption:

More than 90% of students are anxious about the privacy of their keys, which chiefly involves two position in the first situation they do not fully trust the assistance providers because there is no governance about how keys can be used by them and even if the key owner can indeed control their keys on their own and in the second position they trust the service laborer, but keys could be confess if there exists an misbehaving domestic employee or broken server. Therefore encrypting key tuples just like encrypting normal data tuples previously outsourcing seems to be a promising solution to maintaining trust and establish the key owners' control over their own aloofness.

1.3 Key Tuples in Database:

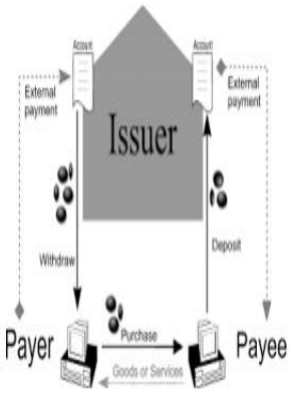
Encrypting key tuples like encrypting data tuples in an all or nobody way [13][14][22] can guarantee the affection and aloofness of keys, but does not contemplate the key authorization and the different privacy compulsion of sensitive attributes in key tuples. Encrypting search keywords (identity characteristic in key tuples) based on searchable symmetric encryption[15][16] or hierarchical declare encryption[27] can guarantee the exploration privacy on key tuples, but does not contemplate the key authorization and the dependence affiliation between existence attributes and key attributes. Encrypting existence attributes and associated identity circumstances in the approach control policy[18][19][26] accomplish the existence and related action privacy of users, but does not contemplate key authorization based on the presence attributes in key tuples and query approval on submitted exploration query. Therefore, in outsourced keys repository, a challenging dispute is to find an encryption arrangement which can encrypt the key tuples in a way that the disparate privacy requirements of conscious attributes in the key tuples can be contented.



To comfortably solve the identified secure problems above, to the finest of our knowledge, we are the first to analyze and present Cloud Key Bank, an cooperative key management framework with imposed privacy and owner administrable authorization described in Section II and compose in Section IV. The awareness of Cloud Key Bank framework is mainly over the following contributions.

1.3 Security effectiveness:

The keys have active ownership because they are used to conserve many other conscious information of the key owner. This associate owner administrable authorization counting key authorization and query approval – only the key owner can determine and control in a fine-grained way who has the rights to approach his/her shared keys through authorization on key aspect (key authorization) and authorization on agree search query (query authorization).



System Architecture of Key

II.EXISTING SYSTEM:

WHILE using online shopping channels, buyer share their purchasing action regarding both goods and account with other potential buyers via appraisal

2.1 Frame work of keys: Cryptographic primeval named Searchable Conditional Proxy Re-Encryption (SC-PRE) which associate the techniques of Hidden Vector Encryption (HVE) and Proxy Re-Encryption (PRE) seamlessly, and introduce a concrete SCPRE design based on actual HVE and PRE schemes.

2.2 Ratings of Keys: The most accepted way for consumers to express their level of comfort with their purchases is through online ratings. The global buyers' satisfaction is assess as the aggregated score of all ratings and is accessible to all potential buyers.

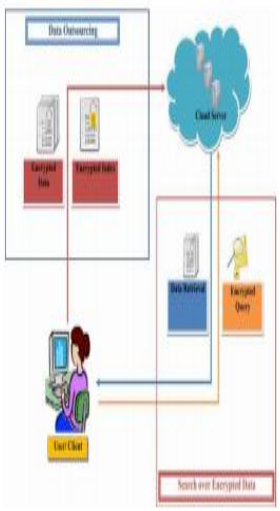
2.2.1 Predicate Reputation: In this paper, we call this amass score for a product its character. The character of a product plays an important role as a guide for possible buyers and significantly control consumers' final purchasing decisions. For example for the key owner, for the delegated user IS the key owner.

2.4 Algorithm:
(CF- BORF-based Venue Selection):
Input: Current User: c, region: R
Output: $Toprec$= A set S' of top-N venues.
Definitions, $V\ e$= set of venues visited by expert user e,
Nc= set of recommended venues,
lc=location of current user c,
$V\ c$ = set of venues visited by current user,
Sr = set of expert users similar to the current user c
ce = closeness measure of the expert user e with the location of current user c
sce is similarity of the user c with the expert user e.
1: $Nc \leftarrow \emptyset$; $zagg \leftarrow \emptyset$;
2: $Sr \leftarrow computsimset$ (c,E)
3: for $each\ e \in Sr$ do
4: S $\leftarrow \{v{:}V\ e|v \notin V\ c\}$
5: $çce \leftarrow ma(computsimD(lc,S))$
6: $zag[e] \leftarrow computeagg(sce\ ,çce)$
7: end for
8: $Nc \leftarrow computRec(c, zagg)$
9: $Toprec \leftarrow sort\ (Nc)$
The privacy keys of the computation with this paper CF-/ BORF.

III. PROPOSED SYSTEM:

The proposed framework, on the other hand, uses all ratings. It evaluates the level of trustworthiness (confidence) of each rating and adjusts the reputation based on the confidence of ratings. We have developed an algorithm that iteratively adjusts a reputation based on the confidence of customer ratings. By adjusting a reputation based on the confidence scores of all ratings, the proposed algorithm calculates the reputation without the risk of omitting ratings by normal users while reducing the influence of unfair ratings by abusers. 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 .So in our proposed system 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. We call this algorithm, which

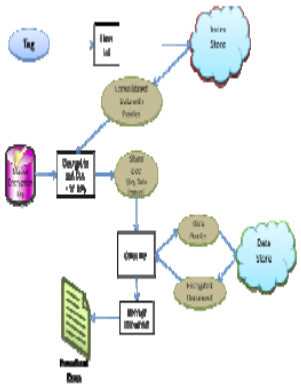
solves the false reputation problem by computing the true reputation, and Filtering.



Architecture Diagram

3.1 True Reputation Scenarios:

1. Measure the activites of user
2. Compute the confidentiality of the keys.
3. Adjusting the areas of transaction



We use an algorthim for finding the transaction using keys. To overcome this we modify the false reputation with true reputation of keys by using encryption and decryption types of integrity and security policy.so the architecture of the true reputation is given.

Bloom filter:-

- Bloom filter maintains the hash table for document replica and query replica.
- Bloom filter reduces the memory storage and search engines efficient and effectively for text retrieval.

Algorithms:-

Constructing Bloom Filters

Consider a set $A = \{a_1, a_2, ..., a_n\}$ of n elements. Bloom filters describe membership information of A using a bit vector V of length m. For this, k hash functions, $h_1, h_2, ..., h_k$ with $h_i : X \to \{1..m\}$, are used as described below:

The following procedure builds an m bits Bloom filter, corresponding to a set A and using $h_1, h_2, ..., h_k$ hash functions:

ProcedureBloomFilter(set A, hash_functions, integer m)
returns filter
filter = allocate m bits initialized to 0
foreach a_i in A**:**
foreachhash function h_j:
filter[$h_j(a_i)$] = 1
endforeach
endforeach
returnfilter

Therefore, if a_i is member of a set A, in the resulting Bloom filter V all bits obtained corresponding to the hashed values of a_i are set to 1. Testing for membership of an

element *elm* is equivalent to testing that all corresponding bits of *V* are set:

ProcedureMembershipTest (elm, filter, hash_functions)
returns yes/no
foreachhash function h_j:
if filter[$h_j(elm)$] != 1 **return** No
endforeach
returnYes

IV-CONCLUSION:

The solution is not so inefficient 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 .So we introduced 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:-

1. Shi, E. and B. Waters, 2008. Delegating Capabilites in Predicate Encryption Systems, Proc. Int'l Colloquium Automata, Languages and Programming (ICALP'08), 5126: 560-578.

2. Iovino, V. and G. Persiano, 2008. Hidden-Vector Encryption with Groups of Prime Order, Proc. Int'l Conf. Pairing-Based Cryptography (Pairing'08), 5209: 75-88.

3. Shen, E., E. Shi and B. Waters, 2009. Predicate Privacy in Encryption Systems, Proc. Theory of Cryptography Conf. (TCC'09), 5444: 457-473.

4. Hwan Park, J., 2011.Efficient Hidden Vector Encryption for Conjunctive Queries on Encrypted Data. IEEE Transactions On Knowledge And Data Engineering, 23(10): 1483-1497.

5. Hwan Park, J., K. Lee, W. Susilo and D.Hoon Lee, 2013. Fully secure hidden vector encryption under standard assumptions. Information Sciences, (232): 188-207.

6. Katz, J., A. Sahai and B. Waters, 2008. Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products.Proc.Theory and Applications of Cryptographic Techniques 27th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT 08), 4965: 146-162.

7. Hacigumus, H., B. Iyer, C. Li and S. Mehrotra, 2002. Executing sql over encrypted data in the databaseservice-provider model. Proc. of the 18th International Conference on Data Engineering(ICDE'02), pp: 216227.

8. Hacigumus, H., B.Iyer, C. Li and S. Mehrotra, 2002. Executing SQL over Encrypted Data in the DatabaseService-Provider Model. Proceedings of the 18th International Conference on Data Engineering(ICDE'02), pp: 216227.