Exchanging Secure Data in Cloud with Owner Authorization and Verification

P.Christopher[1], M. K. Mohamed Faizal[2]
Assistant Professor, Dept of Computer Science and Engineering
M.I.E.T Engineering College, Trichy, Tamilnadu.

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 KeyBank, 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 KeyBank 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. Our experimental results and security analysis show the efficiency and security goals are well achieved.

Keywords- Access Control, Cloud Computing, Protocols, Cryptography.

I. INTRODUCTION

Security and protection indicate huge worries in the appropriation of cloud innovations for information stockpiling. An way to deal with alter these matters is the utilization of encryption. Be that as it may, encryption guarantees the secrecy of the information over the cloud, the utilization of conventional encryption methodologies is not any more effective to bolster the full filling of fine-grained official get to control arrangements (ACPs).With the quick usage of web applications, for example, net managing an account, shopping, interpersonal organizations and information stockpiling dealing with the congestion number of passwords and information encryption keys is turning into a huge trouble for some clients. As pointed out in the survey, security issues are the fundamental association of cloud clients in uses information capacity, which is likewise valid for extended keys stockpiling. Get to in light of encryption has been proposed for in-grained get to control over scrambled information. As appeared in Fig. 1, those gets to gathering information things based on ACPs and encode every gathering with an alternate very much framed key. Clients then are given just the keys for the information things they are conceded to approach. Extensions to abbreviate the quantity of keys that should be appropriated to the clients have been proposed applying requested and other correspondence among information thing. Following three analytical security requirements need to be achieved. Firstly, the keys have high awareness and need to be covered from the honest-but curious service provider and malicious attackers. Secondly, the keys are always reserved with many conscious identity attributes of primary owners and are searched based on them. Thirdly, the keys have strong control because they are used to protect many other conscious information of the key owner.

II. LITERATURE SURVEY

To productively take care of the distinguished secure issues above, to the best of our insight, we are the first to investigate and show CloudKeyBank, a brought together key administration structure with upheld security and proprietor controllable approval portrayed and developed. The acknowledgment of Cloud KeyBank structure is predominantly through the accompanying commitments: To actualize the proposed Cloud KeyBank system, we propose another cryptographic primitive named Searchable Conditional Proxy Re-Encryption (SC- PRE) portrayed , which joins the strategies of concealed vector encryption (HVE) what's more, intermediary re-encryption (PRE) consistently. We too propose a solid SC-PRE plot in view of the existing plans portrayed . SC-PRE effectively explains the test of playing out a key tuple encryption so that the distinctive protection prerequisites of qualities are accomplished in one encryption conspire. In SC-PRE we don't encode every key tuple ti all in all, however first gap each tuple into various quality gatherings, and after that scramble diverse trait aggregates as far as the reliance connection between trait bunches.To accomplish the base data spillage in

the procedure of security and proprietor controllable approval implementation, we presentdouble approval tokens including the Query token and the Delegation token. By utilizing the double approval tokens the key proprietor can encode the Key property amass in such a way that exclusive the client with the suitable tokens can access the common key of key proprietor. The Cloud KeyBank supplier who stores the scrambled key database won't have the capacity to see the substance of the key at whatever time regardless of the possibility that he/she knows all Delegation tokens of the appointed clients. Both the appointed client and the CloudKeyBank supplier cannot infer the private key of key proprietor from the submitted Inquiry token, yet the CloudKeyBank supplier still can perform productive pursuit inquiries by assessing the Query token against each scrambled key tuple.

III. PROPOSED METHODOLOGY

System architecture is the conceptual model that defines the structure, behaviour, and more views of a system. System Architecture is a response to the conceptual and practical difficulties of the description and the design of complex systems. System Architecture helps to describe consistently and design efficiently complex systems. From the above figure 1, contains totally three roles like Data owner, Cloud Server and Search users. Here each and every one has individual roles and all the access in this current model is in form of De-Centralized manner. In the primitive or existing cloud servers, the data access will be obviously in a centralized manner, where the data which is uploaded by owner will be stored inside the cloud server and in turn the access will be in the hands of server itself, But there was no single access control for the owner or user in the current cloud service providers. In this architecture for the first time

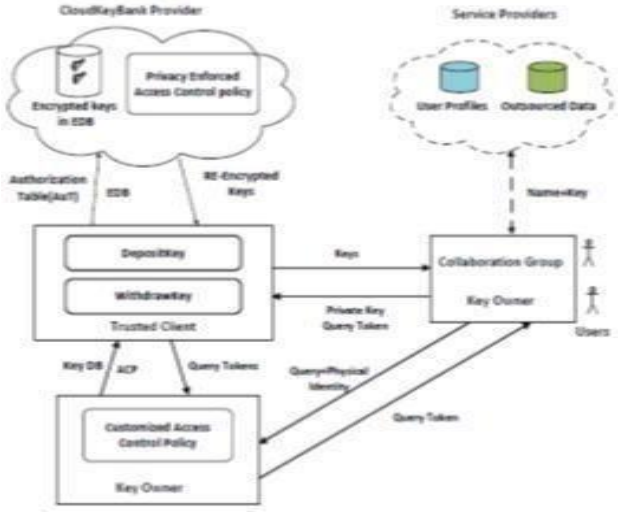

Fig.1: Cloud Key Bank Architecture.

IV. RESULTS AND DISCUSSION

In cryptography, a key-assention convention is a convention whereby at least two gatherings can concur on a key in a manner that both impact the result. In the event that legitimately done, this blocks undesired outsiders from compelling a key decision on the concurring gatherings. Conventions that are valuable by and by additionally don't uncover to any listening in gathering what key has been settled upon. Many key trade frameworks have one gathering create the key, and essentially send that key to the next gathering - the other

V. CONCLUSIONS

To solve the identified critical security requirements for keys outsourcing, we present Cloud KeyBank, the first unified privacy and owner authorization enforced key management framework. To implement Cloud KeyBank, 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

VI. REFERENCES

[1]. CloudKeyBank: Privacy and Owner Authorization Enforced Key Management Framework, Xiuxia Tian, Ling Huang , Tony Wu, Xiaoling Wang ,IEEE Transactions on Knowledge and Data Engineering (Volume:27 , Issue: 12)

[2]. J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Proc of 33th IEEE Symposium on Security and Privacy, pp. 553-567, 2012.

[3]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search, Advances in Cryptography, EUROCRYPT04 , LNCS 3027, pp.506-522, Springer, Berlin, Germany, May 2004.

[4]. Dual-ServerPublic-Key Encryption With Keyword Search for Secure Cloud Storage, Rongmao Chen ,Yi Mu ; Guomin Yang ; Fuchun Guo ; Xiaofen Wang, IEEE Transactionson Information Forensics and Security(Volume:11 , Issue:4)

[5]. X.Boyen and B.Waters, Anonymous hierarchical identity- based encryption (without random oracles). Proceeding of CRYPTO06, 2006.

[6]. E. Shi and B. Waters, Delegating Capabilites in Predicate Encryption Systems,Proc. Intl Colloquium Automata, Languages and Programming (ICALP08), vol. 5126, pp.560-578, 2008.

[7]. H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra. Executing sql over encrypted data in the database-service-provider model. Proc. of the 18th International Conference on Data Engineering(ICDE02), 2002, pp.216- 227.

[8]. V.Pappas, F.Krell, B.Vo, V.Kolesnikov, T.Malkin, S.Geol Choi, W.George, A. D. Keromytis, and S. M. Bellovin. Blind Seer: A Scalable Private DBMS. Proceedings of the 35th IEEE Symposium on Security and Privacy (S and P), San Jose, CA, May 2014.

[9]. N. Shang, F. Paci, M. Nabeel, and E. Bertino. A privacy-preserving approachtopolicy-based content dissemination. Procof the 26th International Conference on Data Engineering(ICDE10), pp. 944-955, 2010.
[10]. M.Nabeel and E.Bertino. Privacy Preserving Delegated Access Controlin Public Clouds. IEEE Transactions On Knowledge And Data Engineering, 26(9):2268-2280,

AUTHOR PROFILE

Christopher is working as an Assistant Professor in M.I.E.T Engineering College, Trichy. He has completed UG and PG under Anna University Chennai. He has 10 years of teaching experience. His areas of interest are Database Management Systems, Web services, Service Oriented Architecture and XML.

M.K.Mohamed Faizal is working as an Assistant Professor in M.I.E.T Engineering College, Trichy. He has completed UG and PG under Anna University Chennai. He has 9.5 years of teaching experience. His areas of interest are Cloud Computing, Computer Networks and Data Structures.