International Journal on Applications in Engineering and Technology
Volume 4: Issue 2: May 2018, pp 48 - 51 www.aetsjournal.com ISSN (Online) : 2455 - 0523

A SURVEY ON BLOCK DESIGN-BASED KEY AGREEMENT FOR GROUP DATA SHARING IN CLOUD COMPUTING

MANIKANDAN, , M.VIJAY ANANTH KUMAR , R.VETRIVENTHAN,
SENTHIL KUMARAN

Abstract— Today, use of cloud computing is rapidly growing for several purposes, mainly for large data storage and sharing data in clouds. Here, users can share data for dynamic groups with cost-effectively. Membership is frequently changing in a cloud. The Existing system is using the protected (secure) commutation channel for data sharing. This implementation is difficult for practice. Still, the existing system is suffering from collusion attack and insecure key distribution with a single cloud. There is no assurance of the data confidentiality and accessibility. In the proposed system, multiple cloud services are used to store data. The System is proposing a safe way for key distribution without using any protected communication channels, and the user can safely get their private keys from group administrators (managers).Any users in the gathering can use the source in the cloud and denied users cannot get to the cloud once more. The system provides fine-grained access control. Also, the system supports the anti-collusion attack with an untrustworthy cloud. Our system is proposing two levels of encryption techniques and a file is stored in a split format on multiple clouds in different groups using a hybrid cloud. The system is providing secure revocation.

Keywords— Key agreement protocol, symmetric balanced incomplete block design (SBIBD), data sharing, cloud computing

I. INTRODUCTION

In cloud computing, the cloud service providers offer single or multiple cloud services for storing and sharing data securely among users i.e. Amazon service S3. Cloud providers offers large storage space with abstraction for simplicity of the user. The membership in the cloud is frequently changing and because of this, security preserving are turned into a challenging issue in the cloud. Company employees in the same department can share and store files in the cloud. However, here is a significant risk to the confidentiality of those stored files. For security purpose, it is necessary to encrypt data before uploading files in the cloud.These schemes do not support for secure data sharing for dynamic groups. Some systems have used techniques for securing data sharing called cryptography among multiple group members in an untrustworthy cloud . But these systems additionally experiences a cost overheads and security risks. These systems are not supported to dynamic group concept.re not supported to dynamic group concept.

1) Background:

In some systems, combined approaches of key policy attribute based encryption, proxy reencryption, and lazy reencryption is used to achieve fine-grained data access control without disclosing data contents. Other system uses the group signatures and cipher text policy attribute based encryption techniques. But these systems does not support to efficient user revocation. It breaches security. The multi owner schemes use the attribute-based techniques. If any owner revokes from an application, it leads to security issues. This approach is not safe for data sharing. Many approaches based on privacy preserving policies in public clouds. These approaches are easily suffering due to collusion attack. The Existing approach supports secure data sharing scheme for dynamic groups in a single cloud. The scheme uses attribute-based techniques. It does not support protected/secure user revocation.The proposed system uses role-based techniques for secure data sharing and key distribution for dynamic groups by taking the advantage of multiple clouds.

In multiple clouds, storage space is again partitioned into groups. The files get partitioned and then store in multiple groups with two level of encryption. The system Supports anti-collision attack and secure user revocation. Our system overcomes cost overhead. Our approach removes a space overhead by using the concept of the virtual storage server. Here, the time and space constraints are applied. If the space of storage became full, stored data is automatically transferred to the virtual server according to the time and space constraint**.**

2) GOALS /OBJECTIVES

System present a novel block design based key agreement protocol that supports group data Sharing in cloud computing. For group data Sharing is used the Structure of a (v,k+1,1) design and multiple participants can be used the common conferences key for participants are derived. And System used the Fault tolerances property marking protocol more practical and secure.

Manikandan , Master of Computer Applications , Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu .

M.Vijay Ananth Kumar , MCA.M.Phil. Assistant professor/MCA **,** Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu .

Mr.R.Vetriventhan , BE , MTech , MISTE , Head of the department , Department of MCA , Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu .

Mr.Senthil Kumaran , ME Phd , Managing Director , Meenaakshi Ramasamy Engineering College , Thathanur , Ariyalur Dt , Tamil Nadu.

II. RELATED WORK

1. "A Secure and Efficient Data Sharing Framework with Delegated Capabilities in Hybrid Cloud" **Author name**: Information Forensics and Security IEEE Transactions on, vol. 10, no. 11, pp. 2381– 2395, 2015.

Abstract—Hybrid cloud is a widely used cloud architecture in large companies that can outsource data to the public cloud, while still supporting various clients like mobile devices. However, such public cloud data outsourcing raises serious security concerns, such as how to preserve data confidentiality and how to regulate access policies to the data stored in public cloud. To address this issue, we design a hybrid cloud architecture that supports data sharing securely and efficiently, even with resource-limited devices, where private cloud serves as a gateway between the public cloud and the data user. Under such architecture, we propose an improved construction of attribute-based encryption that has the capability of delegating encryption/decryption computation, which achieves flexible access control in the cloud and privacy-preserving in data utilization even with mobile devices. Extensive experiments show the scheme can further decrease the computational cost and space overhead at the user side, which is quite efficient for the user with limited mobile devices. In the process of delegating most of the encryption/decryption computation to private cloud, the user can not disclose any information to the private cloud. We also consider the communication security that once frequent attribute revocation happens, our scheme is able to resist some attacks between private cloud and data user by employing anonymous key agreement.

2. An Efficient Protocol For Authenticated Key Agreement" L. Law, A. Menezes, M. Qu, J. Solinas, and S.Vanstone

Abstract-Authentication and key establishment are fundamental building blocks for securing electronic communication. Cryptographic algorithm for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing and key establishment are fit for their purpose. This paper proposes a new and efficient key establishment protocol in the asymmetric (public key) setting that is based on MTI (Matsumoto, Takashima and Imai)-two pass key agreement protocol which consists of three phases; The Transfer and Verification Phase, and The Key Generation Phase. This protocol is strong against most of potential attacks(Known-Key Security ,Forward (Perfect) Secrecy ,Key Compromise Impersonation, Unknown Key-Share Attack ,Small Subgroup Attack, and Man-in-the-Middle Attack) with low complexity (complexity is 4), also it provide authentication between the two entities before exchanging the session keys.

3. "An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data" Mohamed Nabeel, Student Member, I Ning Shang,

Abstract—with the rapid development of cloud computing, cloud storage has been accepted by an increasing number of organizations and individuals, therein serving as a convenient and on-demand outsourcing application. However, upon losing local control of data, it becomes an urgent need for users to verify whether cloud service providers have stored their data securely. Hence, many researchers have devoted themselves to the design of auditing protocols directed at outsourced data. In this paper, we propose an efficient public auditing protocol with global and sampling block less verification as well as batch auditing, where data dynamics are substantially more efficiently supported than is the case with the state of the art. Note that the novel dynamic structure in our protocol consists of a doubly linked info table and a location array. Moreover, with such a structure, computational and communication overheads can be reduced substantially. Security analysis indicates that our protocol can achieve the desired properties. Moreover, numerical analysis and real-world experimental results demonstrate that the proposed protocol achieves a given efficiency in practice.

4. "Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data Storage" Information Forensics and Security IEEE Transactions on, vol. 10, no. 11,

Abstract—Cloud data storage has provided significant benefits by allowing users to store massive amount of data on demand in a cost-effective manner. To protect the privacy of data stored in the cloud, cryptographic role-based access control (RBAC) schemes have been developed to ensure that data can only be accessed by those who are allowed by access policies. However these cryptographic approaches do not address the issues of trust. In this paper, we propose trust models to reason about and improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models provide an approach for the owners and roles to determine the trustworthiness of individual roles and users respectively in the RBAC system. The proposed trust models take into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. We present a design of a trust-based cloud storage system which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes. We have also considered practical application scenarios and illustrated how the trust evaluations can be used to reduce the risks and enhance the quality of decision making by data owners and roles of cloud storage service.

5. "A Decentralized Privacy Preserving Reputation Protocol for the Malicious Adversarial Model" O. Hasan, L.Brunie, E. Bertino, and N. Shang.

Abstract—Users hesitate to submit negative feedback in reputationsystems due to the fear of retaliation from the recipient user.A privacy preserving reputation protocol protects users by hiding their individual feedback and revealing only the reputation score. We present a privacy preserving reputation protocol for the malicious adversarial model. The malicious users in this model actively attempt to

learn the private feedback values of honest users as well as to disrupt the protocol. Our protocol does not require centralized entities, trusted third parties, or specialized platforms, such as anonymous networks and trusted hardware. Moreover, our protocol is efficient. It requires an exchange of messages, where and are the number of users in the protocol and the environment, respectively.

6. D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in Proc. Adv. Cryptol ., 2005, vol. 3621, pp. 258–275.

Abstract: Waters Provable data possession (PDP) is a performance for ensuring the truthfulness of data in storage outsourcing. In this paper, the author address the construction of an efficient PDP scheme for distributed Data storage to support the scalability of service and data migration, in which they consider the continuation of multiple Data service providers to cooperatively store and maintain the clients' data. At hand a cooperative PDP (CPDP) scheme based on homomorphism confirmable response and hash index hierarchy. They prove the security of our scheme based on multi- proverb zeroknowledge proof system, which can satisfy completeness, knowledge soundness, and zero-knowledge properties. In addition, we coherent concert optimization mechanisms for our scheme and in meticulous present a competent method for selecting optimal parameter standards to minimize the totalling costs of clients and storage service providers. Our experiments show that our explanation introduces lower working out and communication operating expense in comparison with noncooperative approaches.

7. *D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," in Proc. 25th Int. Conf. Theory Appl. Cryptographic Tech., 2006, vol. 4004, pp. 573–592.*

Abstract Waters Provable data possession is a procedure for ensuring the integrity of data in outsourcing storeroomservice. In this paper, they propose a cooperative verifiable data possession format in hybrid clouds to bear scalability of service and data migration, in which they deem the existence of multiple Data service providers to cooperatively store up and sustain the clients' data. Our experiments demonstrate that the verification of their scheme requires a small, constant amount of overhead, which minimizes communication complication

8. D. Boneh and M. Naor, "Traitor tracing with constant size Cipher text," in Proc. 15th ACM Conf. Comput.Comm. Security, 2008, pp. 501–510.

Abstract: many storage systems rely on imitation to augment the availability and durability of data on untrusted storage systems. At present, such storage systems provide no strong confirmation that multiple copies of the data are actually stored. Storage Data Servers can conspire to make it look like they are storing many copies of the data, whereas in authenticity they only store a single copy. We address this shortcoming through multiple-replica attestable data possession (MR-PDP): A provably-secure scheme that allows a client that provisions replicas of a file in a storage system to authenticate through a challenge-response etiquette that each unique replica can be shaped at the time of the challenge and that the storage system uses t times the storage required to store a single replica. MRPDP extends previous work on data ownership proofs for a single copy of a file in a client/Data Server storage system. Using MR- PDP to lay up t replicas is computationally much more resourceful than using a single-replica PDP format to store t separate, dissimilar files (e.g., by encrypting each file separately prior to storing it). Another benefit of MR-PDP is that it can generate further replicas on demand, at little expense, when some of the accessible replicas fail

III. EXISTING SYSTEM APPROACH

In existing system the security of key distribution is based on the secure communication channel however to have such channel is a strong assumption and is difficult for practice. To share data while providing privacy-preserving is still a challenging issue, especially for untruth cloud due to collusion attack.

Disadvantages:-

- In existing system we provide single level security
- Fault Detection and fault tolerance problem occur

IV. PROPOSED SYSTEM APPROACH

In Block level Design there are four module owner, user and Admin and Cloud Service Provider. User entry in application First user Register and Login then admin get activated the user and given the token after entre the token user login successfully after login user Search the owner file and cloud Services Provider given the Key in format of KASE. If user Entre the Wrong key (KASE) then level of fault Tolerances is level is increases and that level goes up to 3 then owner known the user information and if owner block the that user then after words user block from particular owner the user are not able to get file of particular owner.

Advantages:

1. The scope of this project is to propose a scheme that provides the anti-collusion data sharing in multiuser cloud.
2. In cloud Computing Fault Detection from user side.
3. In cloud Computing Fault Tolerances and Data Owner.
4. Provide two level securities.
5. Cloud computing reduces the response time and running time of job, also minimizes the risk in deploying application, lowered cost of deployment, and decreasing the effort and increasing innovation
6. Increased Throughput: Cloud makes use of thousands of servers to finish an assignment in reduced time unit verses the time required by a solitary server

V. CONCLUSION

As a development in the technology of the Internet and cryptography, group data sharing in cloud computing has opened up a new area of usefulness to computer networks. With the help of the conference key agreement protocol, the security and efficiency of group data sharing in cloud Computing can be greatly improved. Specifically, the outsourced data of the data owners encrypted by the common conference key are protected from the attacks of adversaries. Compared with conference key distribution, the conference key agreement has qualities of higher safety and reliability. However, the conference key agreement asks for a large amount of information interaction in the system and more computational cost. To combat the problems in the conference key agreement, the SBIBD is employed in the protocol design.

References

[1] "A Secure and Efficient Data Sharing Framework with Delegated Capabilities in Hybrid Cloud " Information Forensics and Security IEEE Transactions on, vol. 10, no. 11, pp. 2381–2395, 2015.
[2] "An Efficient Protocol For Authenticated Key Agreement" L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone
[3] "An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data" Mohamed Nabeel, Student Member, I Ning Shang, Elisa Bertino 2013 IEEE
[4] "Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data" Storage Information Forensics and Security IEEE Transactions on, vol. 10, no. 11, pp. 2381–2395, 2015.
[5] "A Decentralized Privacy Preserving Reputation Protocol for the Malicious Adversarial Model " O. Hasan, L. Brunie, E. Bertino, and N. Shang
[6] "Design of an efficient load balancing algorithm on distributed networks by employing symmetric Balanced incomplete block design" I. Chung and Y. Bae
[7] "Efficient RFID Authentication Scheme with High Security" J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang.