A Survey on A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Anusree Radhakrishnan[1] Minu Lalitha Madhav[2]

[1]PG Scholar, [2]Asst. Professor
Dept. of Computer Science & Engineering , Sree Buddha College of Engineering, Pattoor, Alappuzha, India.

***Abstract -** Cloud provides lower maintenance data sharing among the group members. From this aspect, users can achieve an effective and economical approach for data sharing among group members in the cloud Since the data is of outsourced nature we need to implement some security guarantee in the cloud environment. Since the memberships are changing dynamically so this is an important issue to preserve the privacy, especially for an untrusted cloud due to the collusion attack. Some of the key distribution algorithms are there for giving security in the cloud environment. In the prescribed paper it describes a key distribution method by the help of a key manager. He is in charge of distributing the keys to the members .This paper is a survey on different protocols through which we can implement the cloud computing security concepts*

Keywords: Encryption, decryption, authentication, data security

INTRODUCTION

Cloud computing is a computing feature in which it provides intrinsic data sharing and storage facilities. In cloud computing the organizations don't want to worry about the software and hardware spaces .All the storage concerns are relied on the cloud servers. So the organizations don't want to concerns about the financial overhead. Since we outsource the data to cloud servers there are some issues in the cloud . To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. A cloud is initiated in an environment and more scalable resources need it.

Literature Survey

G Atteneese [1] describes It provide the first efficient solution to delete members from a group without compromising their past signatures or changing the group public key. The security of our mechanism is formally proven, as well as the underlying group signature scheme .Here consider the problem of revocation of identity in group signatures. Group signatures are a very useful primitive in cryptography, allowing a member of a group to sign messages anonymously on behalf of the group. Such signatures must be anonymous and unlinkable, but a group authority must be able to open them in case of dispute. Many constructions have been proposed, some of them are quite efficient. However, a recurrent problem remains concerning revocation of group members. When misusing anonymity, a cheating member must be revoked by the authority, making him unable to sign in the future, but without sacrificing the security of past group signatures. No satisfactory solution has been given to completely solve this problem. Our solution is efficient provided the number of revoked members remains small. It has the advantage that It provide an efficient revocation scheme to delete members from the group without compromising past signatures

In [2] M Backes addresses problem in which a client stores a large amount of data with an untrusted server in such a way that, at any moment, the client can ask the server to compute a function on some portion of its outsourced data. In this scenario, the client must be able to efficiently verify the correctness of the result despite no longer knowing the inputs of the delegated computation, it must be able to keep adding elements to its remote storage, and it does not have to fix in advance (i.e., at data outsourcing time) the functions that it will delegate. Even more ambitiously, clients should be able to verify in time independent of the input-size -- a very appealing property for computations over huge amounts of data. In this work we propose novel cryptographic techniques that solve the above problem for the class of computations of quadratic polynomials over a large number of variables. This class covers a wide range of significant arithmetic computations -- notably, many important statistics. To confirm the efficiency of our solution, we show encouraging performance results, e.g., correctness proofs have size below 1 KB and are verifiable by clients in less than 10 milliseconds.

Paper [3] explains a new system by F Bavo. This system studies various computational and decisional Diffie-Hellman problems by providing reductions among them in the high granularity setting. We show that all three variations of computational Diffie-Hellman problem: square Diffie-Hellman problem, inverse Diffie-Hellman problem and divisible Diffie-Hellman problem, are equivalent with optimal reduction. Also, we are considering variations of the decisional Diffie-Hellman problem in single sample and polynomial samples settings, and we are able to show that all variations are equivalent except for the argument DDH ⇐

SDDH. We are not able to prove or disprove this statement, thus leave an interesting open problem. Keywords: Diffie-Hellman problem, Square Diffie-Hellman problem, Inverse Diffie-Hellman problem, Divisible Diffie-Hellman problem

In [4] K D Bowers describes A proof of irretrievability (POR) is a compact proof by a file system (proved) to a client (verifier) that a target file F is intact, in the sense that the client can fully recover it. As PORs incur lower communication complexity than transmission of F itself, they are an attractive building block for high-assurance remote storage systems. In this paper, we propose a theoretical framework for the design of PORs. Our framework improves the previously proposed POR constructions of Juels-Kaliski and Shacham-Waters, and also sheds light on the conceptual limitations of previous theoretical models for PORs. It supports a fully Byzantine adversarial model, carrying only the restriction---fundamental to all PORs---that the adversary's error rate be bounded when the client seeks to extract F. We propose a new variant on the Juels-Kaliski protocol and describe a prototype implementation. We demonstrate practical encoding even for files F whose size exceeds that of client main memory.

In [5] JianG Zhang tells about mobile cloud computing .It integrates mobile computing and cloud computing .It can greatly extend the boundary of mobile application. Here it uses several cryptographic primitives such as type based proxy re-encryption .The system ensures data security, authentication, privacy, integrity etc. .The system is of light weight. And it uses minimum number of resources .No trusted third party is involved here. The system uses the concept of Merkle Hash Tree(MHT) for the dynamic operation simplicity. It has the disadvantage of the tree implementation complexity.

Conclusion

This survey has been performed for collecting the details of different protocols / mechanisms for implementing Mobile cloud computing. Mobile cloud computing is a facility that can be used by many of the users in order to solve the problem of data storage. But when we integrate the cloud concept to the mobile technology. Through this survey a number of different technologies are identified and studied. But no method can be said as perfect one. But cloud has to satisfy several security parameters such as integrity, authorization, access control etc. MCC is an emerging technology which is used by most of the users and it is needed to ensure the security mechanism with all concerns.

Acknowledgments

We are grateful to our project guide and PG Coordinator Prof. Minu Lalitha Madhavu for her remarks, suggestions and for providing all the vital facilities like providing the Internet access and important books, which were essential. We are also thankful to all the staff members of the Department.

REFERENCES

[1] G. Ateniese, J. Camenisch, M. Joye, And G. Tsudik. “Efficient Revocation In Group Signatures”. In M. Bellare, Editor, Crypto ’2015, Volume 1880 Of Lncs, Pages 255–270. Springer-Verlag, 2015

[2] Verifiable Delegation Of Computation On Outsourced Data - M. Backes, D. Fiore, And R. M. Reischuk, Editor, Crypto ’2015, Volume 1880 Of Lncs, Pages 255–270. Springer-Verlag, 2015

[3] Variations Of Diffie-Hellman Proble - F. Bao, R. Deng, And H. Zhu

[4] Proofs Of Retrievability: Theory And Implementation - K. D. Bowers, A. Juels, And A. Oprea

[5] Jiang Zhang, Zhenfeng Zhang, and Hui Guo “Towards Secure Data Distribution Systems in Mobile Cloud Computing” , Annual IEEE Int. Conf. on Local Computer Networks