Volume 6, Issue 3, March 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Data Sharing in Cloud without Certificate Verification Processs Using Id-Based Proxy Ring Signature

[1]A. Selvakumar, [2]R. Janani, [3]R. Kanimozhi, [4]R. Karthika

[1]CSE & Assistant Professor, [2, 3, 4] CSE & Student

[1, 2, 3, 4] Christ College Engineering & Technology, Karnataka, India

Abstract-Data sharing has never been easier with the advances of cloud computing. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. A ring signature is a simplified group signature without any manager. It protects the anonymity of a signer. Unlike the group signature schemes the ring signature scheme requires neither a group manager, nor a setup procedure, nor the action of non-signing members. This signature does not reveal the identity of the signer but it may be varied with this signature that the signer belong to the possible signers set. There is no revocation manager. This allows unconditional anonymity of signer. Therefore, we introduce proxy signature scheme to allow a proxy signer to sign on behalf of an original signer. We can achieve the singer ambiguity and key secrecy. To achieve user account security, we employee authentication process. In this authentication process user thump impression is capture and compared with the user data which are stored in database during registration process.

Keywords— Ring signature, revocation manager, data integrity, anonymity.

I. INTRODUCTION

Cloud systems can be used to enable data sharing capabilities and this can provide an abundant of benefits to the user. There is currently a push for IT organizations to increase their data sharing efforts. According to a survey by InformationWeek , all the organizations shared their data 74 % sharing with customers and 64 % sharing with suppliers. A fourth of the surveyed organizations consider data sharing a top priority. The benefits organizations can gain from data sharing is higher productivity. With multiple users from different organizations contributing to data in the Cloud, the time and cost will be much less compared to having to manually exchange data and hence creating a clutter of redundant and possibly out-of-date documents.

Due to its openness, data sharing is always deployed in a hostile environment and vulnerable to a number of security threats. Taking energy usage data sharing in Smart Grid as an example, there are several security goals a practical system must meet, including: Data Authenticity, Anonymity and Efficiency.

II. SCOPE OF THE PROJECT

A user can easily share the date within the group and provide maximum security for the entire group. Group manager can easily revoke the unwanted members in the group. The proxy signature will enhance all the security issues in a group This will be useful for all the public and private sectors.

III. RELATED WORKS

The review articles and surveys presented in this section do not focus specifically on secure data sharing in the Cloud, rather the main requirements that will enable it. The study of secure data sharing in the Cloud is fairly new and has become increasingly important with the advancements and growing popularity of the Cloud as well as the growing need to share data between people. We categorise the existing review articles in two aspects: data sharing and Cloud security.

There have been a number of reviews on security and privacy in the Cloud identifies the five concerns of Cloud computing; confidentiality, integrity, availability, accountability, and privacy and thoroughly reviews the threats to each of the concerns as well as strategies. A survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security breaches of one's personal data in the Cloud. They then carry out analysis work on the measurements to check whether SaaS complies with privacy and security standards. The method does not however take into account other Cloud models such as Platform As-A-Service (PaaS) and in particular Infrastructure-As-A-Service (IaaS), as needed for data sharing. A survey on a number of users to determine the user experience of Cloud computing and found that the main issue of all users was trust and how to choose between different Cloud Service Providers . "Although researchers have identified numerous security threats to the Cloud, malicious insiders still represent a significant concern." The impact of the Internet on data sharing across many different organisations such as government agencies and businesses. They classify data sharing into data dissemination, query restriction, and record matching. They also provide a framework for secure and useful sharing of data on the internet.

IV. SYSTEM ANALYSIS

A. Existing Work:

Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. The ability to access, and respond to much more precise and detailed data from all levels of the electric grid is critical to optimal energy usage. Due to its openness, data sharing is always deployed in a open environment and weakness to a number of security threats. If user desire to revoke from the group it's not possible in my existing system.

B. Drawbacks in Existing System:

- It is difficult to provide security.
- It is critical to efficient energy usage.
- Data integrity is low.
- User information reveal to others.
- User cannot join other group, if he/she is member of any group.
- There is no revocation manager. This lead to unconditional anonymity of signer.

C. Proposed System:

We introduced proxy based ring signature to achieve sing ambiguity and key secrecy. In this signature, we have to do three steps which are given below:

- Proxy Key Generation
- Verification

The original signer prepares a warrant, which is explicit description of the delegation relation. Then he sends to the proxy group. Each proxy signer uses his secret key to sign the warrant and gets his proxy key. Proxy Ring Signing for signing any with signers's public key. In verification process given message, its ring signature, and the set of the identities of all ring members, the verifier can check the validity of the signature. In this we also capture the user thumb impression for authentication purpose to achieve account security.

D. Proposed System Advantages:

- It is easy to provide security.
- A practical system must reduce the computation and communication cost as much as possible.
- There is no costly certificate verification process.
- User privacy is maintained.
- Data Integrity is achieved
- User can join other group, by revoking the existing group.
- Singer ambiguity.
- Key secrecy.

V. SYSTEM ARCHITECTURE

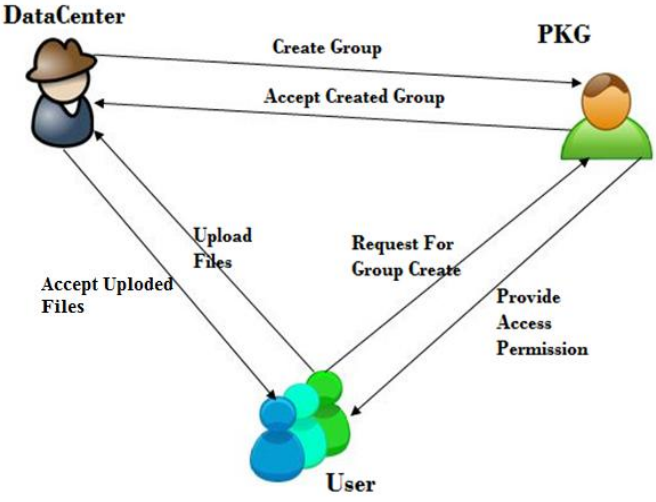

Fig 1: Block diagram of proposed system

VI. MODULE DESCRIPTION

Module 1: Key Secrecy:

In computing user P_i's private key S_i from the corresponding public key $PK_o + PK_{Pi}$ requires the knowledge of original signer's private key so and proxy signer's private key s_{pi} . According to definition these keys are protected under the intractability of DLP in G1 as $PK_o = s_oP$ and $PK_{Pi} = s_{pi}P$.

Signer ambiguity a valid proxy ring signature (c_1, c_2,……c_n, T) with proxy group L0 generated by PS_i all c_i's are computed. Since T_i ε G_1 is chosen uniformly at random, each ci is uniformly distributed over G_2. Thus, regardless who the actual signer is and how many ring members involved (c_1, c_2,….., c_n) biases to no specific ring member. Other discussions are very similar as in previous sections.

Module 2: Proxy key generation:

This pkg is more useful in order to generate a secrete key to our mail and using that key only we can login into our group. The key consist of characters and numbers which will be more strong enough to hack the key. These key are one time key generated for every user so it cannot be use it again it will enhance the security of group. Using this type generation we can easily safe guard our group details from the attacker.

Module 3: Group manager:

Group manager has the power to add or revoke the user from the group. If he found that the group is traced by some other unauthorized person then he will easily revoke the user from the group. He will monitor the each and every moment of the group member activities which is more useful to find in which way the data are leaked. He only can give the rights to access the level of data.

VII. CONCLUSIONS

In this paper we proposed a new proxy ring signature scheme and authentication process which, whenever proxy signer want to sign message on behalf of the original signer provide anonymity and provide user account security. The proposed scheme is more efficient than the scheme of Zhang et al.'s, especially for the pairing operation required in the signature verification. This proxy ring signature scheme is more efficient for those verifiers who have limited computing power.

ACKNOWLEDGMENT

I would like to express my thanks to the people who helped me most throughout my project. I am grateful to my guide for nonstop for the project. A special thanks of mine goes to my project members who helped me out in completing my project, where they all exchanged their own ideas, thoughts and made this possible to complete my project with all accurate information. I wish to thank my parents of their personal support or attention who inspired me to go my own way. At last but not the least I want to thank my friends who treasured me for my hard work and encouraged me and finally to God who made all the things possible for me till the end.

REFERENCES

[1] M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n Signatures from a Variety of Keys. In ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 415–432. Springer, 2002.

[2] R. Anderson. Two remarks on public-key cryptology. Manuscript, Sep. 2000. Relevant material presented by the author in an invited lecture at the Fourth ACM Conference on Computer and Communications Security, 1997.

[3] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In CRYPTO 2000, volume 1880 of Lecture Notes in Computer Science, pages 255–270. Springer, 2000.

[4] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong. Id-based ring signature scheme secure in the standard model. In IWSEC, volume 4266 of Lecture Notes in Computer Science, pages 1–16. Springer, 2006.

[5] A. K. Awasthi and S. Lal. Id-based ring signature and proxy ring signature schemes from bilinear pairings. CoRR, abs/cs/0504097, 2005.

[6] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of group signatures: formal definitions, simplified requirements and a construction based on general assumptions. In EUROCRYPT'03, volume 2656 of Lecture Notes in Computer Science. Springer, 2003.

[7] M. Bellare and S. Miner. A forward-secure digital signature scheme. In Crypto'99, volume 1666 of Lecture Notes in Computer Science, pages 431–448. Springer-Verlag, 1999.