Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.1088 – 1094

RESEARCH ARTICLE

Anonymously Share Data on Group Signature in the Large Groups of Cloud

Rengasamy.R[1], Guru Rani.G[2]

[1]PG Student, Department of CSE & N.P.R College of Engg and Tech, Dindigul, Tamil Nadu, India
[2]Assistant professor, Department of CSE & N.P.R College of Engg and Tech, Dindigul, Tamil Nadu, India
[1] rengasamy31@gmail.com; [2] ranitcguru@yahoo.com

Abstract— ***we have a tendency to propose a secure multi-owner information sharing theme. It implies that any user within the cluster will firmly share information with others by the untrusted cloud. Our planned theme is in a position to support dynamic teams expeditiously. Specifically, new granted users will directly decipher information files uploaded before their participation while not contacting with information homeowners. User revocation is often simply achieved through a unique revocation list while not change the key keys of the remaining users. The dimensions and computation overhead of encoding area unit constant and freelance with the amount of revoked users. We offer secure and privacy-preserving access management to users that guarantees any member during a cluster to anonymously utilize the cloud resource. Moreover, the $64000 identities of knowledge homeowners are often disclosed by the cluster manager once disputes occur. We offer rigorous security analysis, and perform intensive simulations to demonstrate the potency of our theme in terms of storage and computation overhead.***

Keywords— ***Revocation; Revoke; Signature (CDA); Data Aggregation; Symmetric key encryption***

I. Introduction

First, identity privacy is one in every of the foremost vital obstacles for the wide readying of cloud computing. While not the guarantee of identity privacy, users is also unwilling to affix in cloud computing systems as a result of their real identities might be simply disclosed to cloud suppliers and attackers. On the opposite hand, unconditional identity privacy could incur the abuse of privacy. As an example, misbehaved employees will deceive others within the company by sharing false files while not being traceable. Therefore, traceability, that allows the cluster manager (e.g., an organization manager) to reveal the $64000 identity of a user, is additionally extremely fascinating. Second, it's extremely counseled that any member in an exceedingly cluster ought to be able to totally relish the information storing and sharing services provided by the cloud, that is outlined because the multiple-owner manner. Compared with the single-owner manner, Where ever solely the cluster manager will store and modify knowledge within the cloud, the multiple-owner manner is additional versatile in sensible Applications. More concretely, every user within the cluster browser to not solely read knowledge, however additionally modify a part of knowledge within the entire record shared by the corporate. Last however not least, teams are ordinarily dynamic in follow, e.g., new employees participation and current worker revocation in an exceedingly company. The changes of membership build secure knowledge sharing extraordinarily troublesome. On one hand, the anonymous system challenges new granted users to find out the content of information files hold on before their participation, as a result of it's not possible for brand new granted users to contact with anonymous knowledge house owners, and procure the corresponding decoding keys. On the opposite hand, AN economical membership revocation mechanism while not change the key keys of the remaining users is additionally desired to attenuate the complexness of key management. Many security schemes for knowledge sharing on untrusted servers are projected. In these approaches, knowledge house owners store the encrypted knowledge files in untrusted storage and distribute the corresponding decoding keys solely to approved users. Thus, unauthorized users furthermore as storage servers cannot learn the content of the information files as a result of they need no information of the decoding keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the quantity of information house owners and also the number of revoked users, severally. By setting a gaggle with one attribute, Lu et al. projected a secure birthplace theme supported the cipher text-policy attribute-based secret writing technique, that permits any member in an exceedingly cluster to share knowledge with others. However, the difficulty of user revocation isn't self-addressed in their theme. Yu et al. bestowed a scalable and fine-grained knowledge access management theme in cloud computing supported the key policy attribute-based secret writing (KP-ABE) technique. Owner manner hinders the adoption of their theme into the case, wherever any user is granted to store and share knowledge.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the multi group data sharing techniques and security mechanism used on data aggregation. Section III involves the detailed description about the proposed method. Section IV presents the performance analysis. This paper concludes in Section V.

II. **RELATED WORK**

This section deals with the works related to the Data Aggregation techniques and the security mechnasims used for secure transmission.*Chien-Minget al* proposed a recoverable concealed data aggregation technique for data integrity. The system provides better secure transmission between the base station and the individual user[1].*Westhoff et al* presented a Malleability Resilient Concealed Data Aggregation (MR-CDA). This approach combines homomorphic MACs with additively homomorphic encryption tachniques. It helps to detect the outside attackers which maliciously add resp inject encrypted data to an aggregated encrypted data format [2].*Ozdemir et al* designed a hierarchial concealed data aggregation protocol that allows the aggregation of data packets that are encrypted with different encryption keys. During the decryption, the base station was able to classify the encrypted and aggregated data based on the encryption keys. An eliptic curve cryptography based homomorphic encryption algorithm was presented to offer data integrity and confidentiality along with the hierarchial data aggregation[3]. *Yue-Hsun et al*proposed a sorting scheme on ciphertexts without decryption; where ciphertexts were generated by Elliptic Curve Eigamal encryption. This method preserves assitive homomorphic property of the Curve Eigamal encryption[4].*Huang et al*proposed a secure encrypted data aggregation method. This method eliminates the redundant sensor readings without using encryption and privacy during transmission. This technique was resilient to known-plaintext attacks, chosen-plaintext attacks, cipher text-only attacks and man-in-the middle attacks [5].*Dezfouli et al* proposed a protocol for concealed data aggregation. Here, the network was divided into virtual cells. Nodes within each cell produce a shared key to send and receive the concealed data with each other [6].*Roy et al* proposed an aggregation framework which combines multipath routing schemes with supplicate insensitive algorithms to accurately compute the aggregate messages. Also, a light weight verification algorithm was presented. Here, the base station can determine if the computed aggregate includes any false contribution [7]. *Applebaum et al*proposed a privacy-preserving data aggregation among a large number of participants. Here, scalability and efficiency was achieved through a 'semi-centralized architecture that divides responsibility between a proxy and a database. The cryptographic protocol protects the privacy of both the participants and the keywords[8].*Li et al* proposed an energy efficient and high accuracy scheme for secure data aggregation. The accurate data aggregation was achieved without releasing private sensor readings and without introducing significant overhead on the battery-limited sensors [9].*Chu et al*proposed a Receiver-Bounded Online/Offline Identity-based Encryption (RB-OOIBE). The encryption process was splitted into two parts. One is offline part, where all heavy computations were done without the knowledge of the receiver's identity and the plaintext message. Another one is the online stage, where only light computations such as modular operation and symmetric key encryption were required combined with the receiver's identity and the plaintext message. Each offline cipher text can be reused for the same receiver [10].*Rasmi et al* presented a paired cipher text public key system based on RSA. This method incorporates two hard mathematical problems like discrete logarithms and factoring to provide secure transmission. *Peng et al* proposed an index structure that supports cipher text indexing and retrieval. It allows full-text search on the encrypted documents in multiple formats without decryption. *Hohenberger et al* proposed a method for craeting chosen ciphertext secure encryption. The focal point of this method was discovering a new abstarction called Detectable Chosen Ciphertext Security (DCCA).*Agrawal et al* presented a detailed study of most of the symmetric encryption techniques with their advantage and limitations. Li *et al* proposed a lightweight scheme for secure sensor association a key management in Body Area Networks (BAN). A different kind of secret keys was generated on demand after deployment. The Group Device Pairing (GDP) supports batch deployment of sensor nodes to save setup time. This system does not depend on any additional hardware devices and it was based on symmetric key cryptography.

III. **MULTI** OWNER: SECURE DATA SHARING IN CLOUD APPLICATIONS

The proposed system called secure sharing-MA, which provides data sharing between multiple groups. There are three part of work to implements in the proposed system. An adversary can deduce the key from only the encrypted messages. RCDA-MA realizes the aggregation query in Database, which is a trusted service provider. To secure the database a symmetric key scheme is used. The cipher texts for the entire transmission are implemented by using two points of different orders. So, the effect of one point can be removed by multiplying the aggregated cipher text with the order of the point and then the scalar of other point can be obtained. The proposed model provides secure communication and data transmission from Base Station to individual users.

The following sections are briefly addressing the delivery of group public keys to sensor nodes with security criteria's.

A. *Setup Phase*

The entire data sharing is divided into key base; each key has one group key to aggregate the outcome of the other data present in the corresponding group. There are two approaches are incorporated to set up the data sharing for key distribution: One is Key Pre-distribution and the other one are Key Post-distributive.

Key Pre-distribution

The necessary keys and functions are preloaded into the data sharing. Each node is assigned with a symmetric key. So that, they can work correctly after being spread out over a geographical region.

Key Post-distribution

The sensor nodes are capable of nothing about keys, before Data transmission among multi group in the cloud need to follow the following steps:

User in the group can securely share data with others by the untrusted cloud. The real identities of data owners can be revealed by the group manager. User needs to compute a group signature for his/her authentication. Mona is secure for access control, data confidentiality, anonymity and traceability. Cloud is operated by CSPs and provides priced abundant storage services. The cloud is not fully trusted by users. The group manager is acted by the administrator of the company. Its role is Key generation, user registration, user revocation. The staffs play the role of group members. The users store the private data in the cloud and share the group users. Symmetric signature algorithm to solve the secure data sharing in multi group.

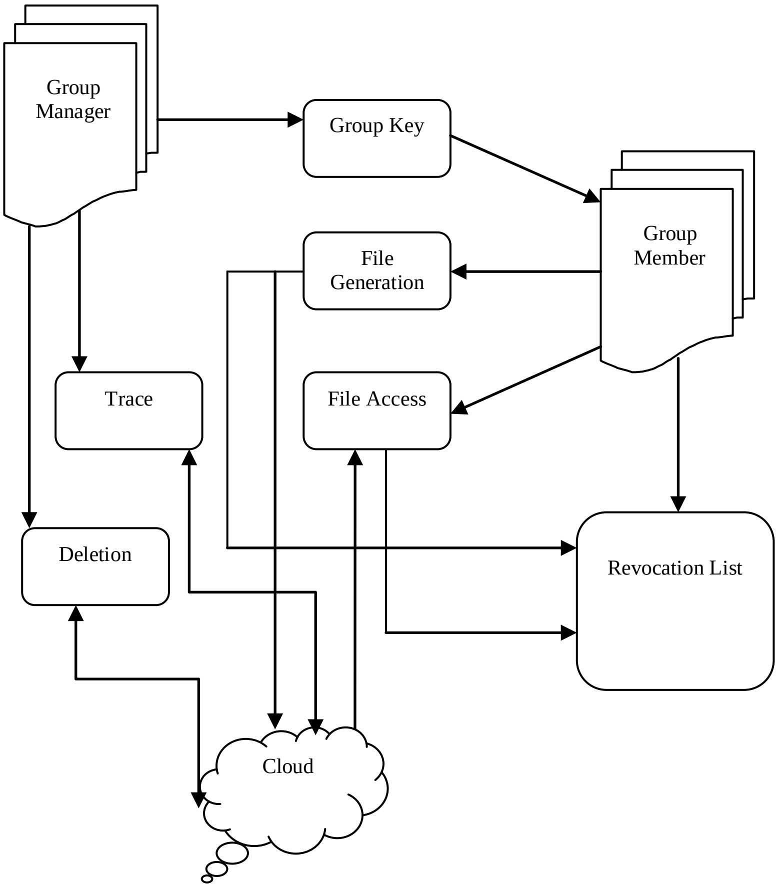

Fig.1. Flow for Secure Transmission

B. ***Symmetric Key Algorithm Steps***

```
DESCryptoServiceProvider key = new DESCryptoServiceProvider ();
Byte [] buffer;
// create a memory stream.
MemoryStream ms = new MemoryStream ();
// create a CryptoStream using the memory stream and the CSP DES key
CryptoStream crypstream = new CryptoStream (ms, key.CreateEncryptor (), CryptoStreamMode.Write);
// create a StreamWriter to write a string to the stream.
StreamWriter sw = new StreamWriter (crypstream);
// Write the strText to the stream.
 sw.WriteLine (strText);
 // Close the StreamWriter and CryptoStream.
 sw.Close ();
crypstream.Close ();
// Get an array of bytes that represents the memory stream
byte [] buffer = ms.ToArray();
// Close the memory stream.
ms.Close ();
// Return the encrypted byte array.
return buffer;
```

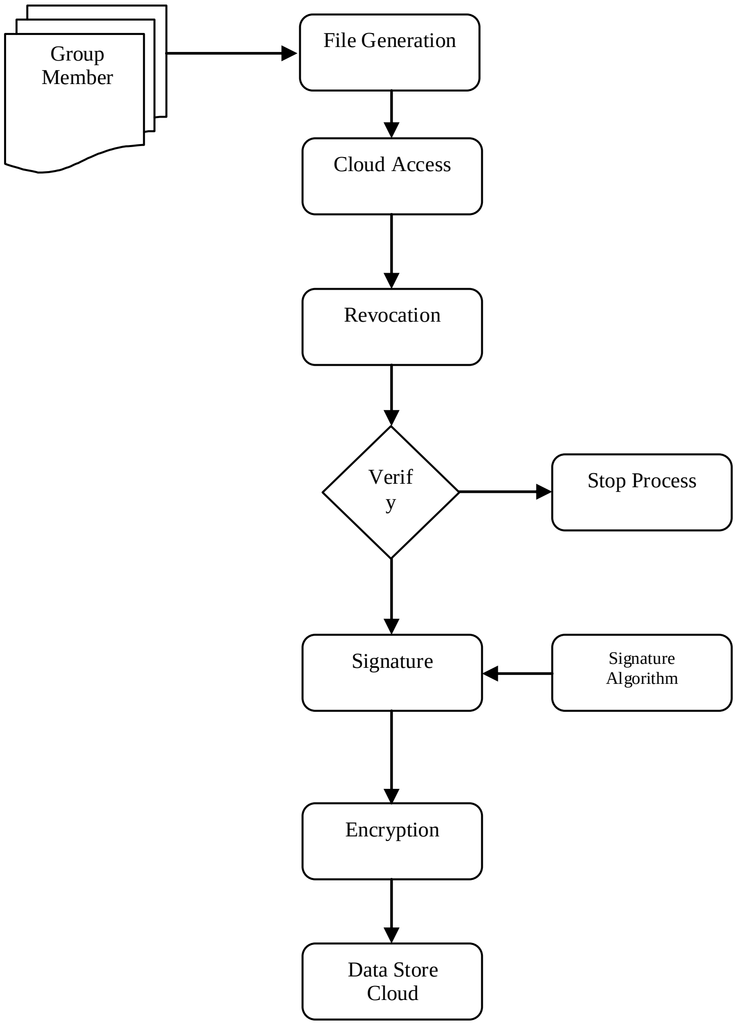

Fig. 1 Example of Group member Secure Sharing

Symmetric Encryption Algorithm

Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. This is also known as private key encryption.

C. Signature Generation and Verification

Signature Generation

Choose an approved cryptographic hash function H. In the original DSS, H was always SHA-1, but the stronger SHA-2 hash functions are approved for use in the current DSS. The hash output may be truncated to the size of a key pair. Decide on a key length L and N. This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1024 (inclusive). Choose an N-bit prime q. N must be less than or equal to the hash output length. Choose an L-bit prime modulus p such that p–1 is a multiple of q. Choose g, a number whose multiplicative order modulo p is q.

Let **H** be the hashing function and ***m*** the message:

- Generate a random per-message value **k** where 0 < k < q
- Calculate $r = (g^k \bmod p) \bmod q$
- In the unlikely case that $r = 0$, start again with a different random k
- Calculate $s = k^{-1}(H(m) + xr) \bmod q$
- In the unlikely case that $s = 0$, start again with a different random k
- The signature is (r, s)

The first two steps amount to creating a new per-message key. The modular exponentiation here is the most computationally expensive part of the signing operation, and it may be computed before the message hash is known. The modular inverse $k^{-1} \bmod q$ is the second most expensive part, and it may also be computed before the message hash is known. It may be computed using the extended Euclidean algorithm or using Fermat's little theorem as $k^{q-2} \bmod q$.

Signature Verification

- Reject the signature if $0 < r < q$ or $0 < s < q$ is not satisfied.
- Calculate $w = s^{-1} \bmod q$
- Calculate $u_1 = H(m) \cdot w \bmod q$
- Calculate $u_2 = r \cdot w \bmod q$
- Calculate $v = ((g^{u_1} y^{u_2}) \bmod p) \bmod q$
- The signature is valid if $v = r$

DSA is similar to the ElGamal signature scheme.

D. Performance Analysis

This section presents the performance evaluation of the proposed Multi owner data sharing. The performance is evaluated based on the following measures:

Aggregation accuracy

The accuracy metric is defined as the ratio between the collected summations by the data sharing scheme used and the real summation of all the individual sensor nodes.

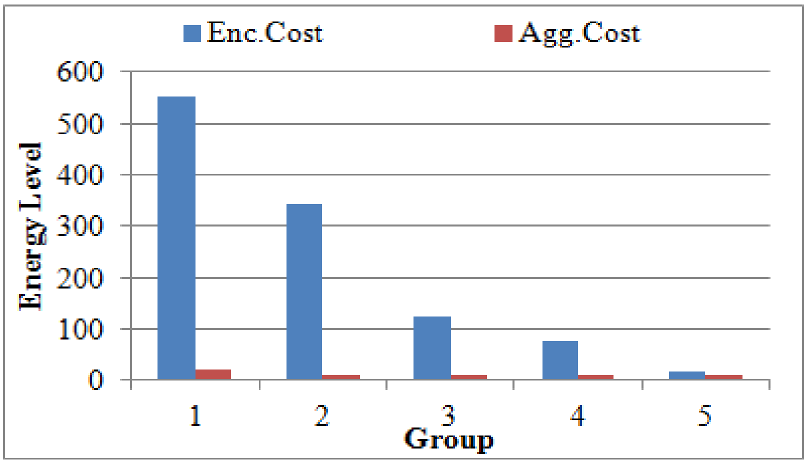

Fig.3. Energy level for encryption cost and sharing cost

IV. CONCLUSIONS

With the character of low maintenance, cloud computing provides a cost-effective and economical answer for sharing cluster resource among cloud users. sadly, sharing information during a exceedingly in a very multi-owner manner whereas conserving information and identity privacy from an untrusted cloud continues to be a difficult issue, as a result of the frequent amendment of the membership. During this paper, we tend to propose a secure multi owner information sharing theme, named Mona, for dynamic teams within the cloud. By investing cluster signature and dynamic broadcast secret writing techniques, any cloud user will anonymously share information with others. Meanwhile, the storage overhead and secret writing computation price of our theme area unit freelance with the quantity of revoked users. Additionally, we tend to analyze the safety of our theme with rigorous proofs, and demonstrate the potency of our theme in experiments. In future, this approach is extended with the privacy preserving data sharing aggregation methodology in the cloud storage.

REFERENCES

[1] C. Chien-Ming, L. Yue-Hsun, L. Ya-Ching, and S. Hung-Min, "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, pp. 727-734, 2012.

[2] D. Westhoff and O. Ugus, "Malleability resilient (premium) Concealed Data Aggregation," in World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a, 2013, pp. 1-6.

[3] S. Ozdemir and Y. Xiao, "Integrity protecting hierarchical concealed data aggregation for wireless sensor networks," Computer Networks, vol. 55, pp. 1735-1746, 2011.

[4] L. Yue-Hsun, H. Bing-Zhe, S. Hung-Min, and C. Yen-Hsueh, "CDS: Concealed data sorting scheme in wireless sensor networks," in Computer Symposium (ICS), 2010 International, 2010, pp. 370-375.

[5] S.-I. Huang, S. Shieh, and J. Tygar, "Secure encrypted-data aggregation for wireless sensor networks," Wireless Networks, vol. 16, pp. 915-927, 2010.

[6] M. A. Dezfouli, S. Mazraeh, and M. Yektaie, "The New Method of Concealed Data Aggregation in Wireless Sensor: A Case Study," World Academy of Science, Engineering and Technology, vol. 60, 2011.

[7] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," Information Forensics and Security, IEEE Transactions on, vol. 7, pp. 1040-1052, 2012.

[8] B. Applebaum, H. Ringberg, M. J. Freedman, M. Caesar, and J. Rexford, "Collaborative, privacy-preserving data aggregation at scale," in Privacy Enhancing Technologies, 2010, pp. 56-74.

[9] H. Li, K. Lin, and K. Li, "Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks," Computer Communications, vol. 34, pp. 591-597, 2011.

[10] C.-K. Chu, J. K. Liu, J. Zhou, F. Bao, and R. H. Deng, "Practical ID-based encryption for wireless sensor network," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 337-340.