ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Secure Data Sharing for Dynamic and Large Groups in the Cloud

M.R. Kalai Selvi[1]

M.E CSE, Oxford Engineering College, Pirattiyur, Trichy-9, Tamilnadu, India[1]

ABSTRACT- Cloud computing provides resources of the computing infrastructure as services over the internet as well as it provide solution for sharing group resource among group members. Unfortunately, designing a secure data sharing scheme for multi-owner groups in the cloud is not an easy task, due to the identity privacy and the frequent change of the membership. By the first efficient group signature and dynamic broadcast encryption techniques, any group member can share data with others in the cloud. The efficient first group signature scheme whose public key and signatures have length independent of the number of group members and which can therefore also be used for large groups. The computational effort for signing and verifying, independent of the number of group members. Since, the computation overhead of encryption operations and storage overhead is reduced as well as it is independent with the number of revoked user. Moreover, the storage overhead and conjointly the secret writing computation worth are reduced. Thorough analysis show that planned theme satisfies the desired security needs and guarantees efficiency as well.

KEYWORDS- Cloud computing, privacy-preserving, dynamic groups, encrypt-on-disk, secure provenance.

I. INTRODUCTION

Cloud Computing is new class of network based totally computing that takes place over the internet. It is recognized as an alternate to ancient data technology due to its intrinsic resource-sharing and low-maintenance characteristics. Cloud Computing uses the online for communication and provides varied services to cloud users with the help of powerful datacenters. By migrating the native information management systems into cloud servers, users can relish high-quality services and save necessary investments on their native infrastructures.

One altogether the essential services offered by cloud suppliers is data storage. Specially, the cloud servers managed by cloud suppliers don't seem to be completely trustworthy by user whereas the knowledge files keep inside the cloud might even be sensitive and confidential, like business plans. To preserve data confidential and privacy, a basic resolution is to jot down data files, thus transfer the encrypted data into the cloud. Sadly, turning out with associate economical and secure information sharing theme for groups inside the cloud is not a straightforward task due to the following troublesome issues.

- Identity privacy is one altogether the foremost necessary obstacles for the wide activity of cloud computing. Whereas not the guarantee of identity privacy, users might even be unwilling to hitch in cloud computing systems as a results of their real identities could be merely disclosed to cloud suppliers and attackers.
- It is extraordinarily prompt that any member in a passing cluster needs to be ready to completely get pleasure from the knowledge storing and sharing services provided by the cloud, that's printed as a result of the multiple-owner manner. Whereas in the single-owner manner, where solely the cluster manager can store and modify information inside the cloud, the multiple-owner manner could be a heap of versatile in smart applications.
- Groups are typically dynamic in follow. The changes of membership build secure information sharing very powerful.

Types of Cloud Services:

- *Software as a Service*- Software as a Service choices a whole application offered as a service on demand. One instance of the software runs on the cloud and services multiple finish users or consumer organizations.
- *Platform as a Service*- PaaS provides the entire infrastructure required to develop and run applications over the web. Users will access custom apps in-built the cloud, similar to their SaaS apps, whereas IT departments and ISVs will specialize in innovation rather than complicated infrastructure. By leverage PaaS, organizations will send a major portion of their budgets from "keeping the lights on" to making applications that offer real business worth.
- *Infrastructure as a Service*- Infrastructure-as-a-Service (IaaS) represents a brand new consumption model for the employment of IT resources. An IaaS supplier offers customers information measure, storage associated calculate power on an elastic, on-demand basis, over the web. IaaS' alternative key edges embody improved income, accommodation of wide inaccurate provision coming up with, and exceptional transparency in utilization and prices.

Types of Clouds:

- Private Cloud- Typically owned by the respective enterprise and/or leased.
- Public Cloud- When a cloud is made available in a pay-as-you-go manner to the general public, we call it a public cloud; the service being sold is utility computing.
- Hybrid Cloud- It consist of a mixed employment of private and public cloud infrastructure so as to achieve a maximum of cost reduction through outsourcing whilst maintaining the desired degree of control over.

II. RELATED WORK

In [4], Kallahalla et al. planned a cryptologic storage system that permits secure file sharing while not putting a lot of trust on untrusted servers, named Plutus. Plutus groups files into Filegroups. With Filegroups, all file with identical sharing attributes are classified within the same filegroup and are protected with the same key. Encrypting every filegroup with a novel file-block key, the information owner will share the filegroups with others through delivering the corresponding lockbox key; wherever the lockbox secret is accustomed encode the file-block keys. However, it brings a couple of significant key distribution overhead for large-scale file sharing. In addition, the file-block key must be updated and distributed once more for a user revocation.

In [5], Sirius assumes the network storage is untrusted and provides its own read-write cryptographic access management for file level sharing. The goal of Sirius is to secure information placed on any untrusted and unrestricted network digital computer whereas maintaining performance and standard file system linguistics. Files keep on the file server are unbroken in two components. One half contains the file meta knowledge and therefore the different the file data. The file meta knowledge contains the access management data whereas the file data contains the encrypted and signed contents. Every of that is encrypted below the general public key of approved users. Thus, the dimensions of the file data are proportional to the amount of approved users. The user revocation within the theme is an uncontrollable issue particularly for large-scale sharing, since the file data must be updated.

Ateniese et al. [6] leveraged proxy reencryptions to secure distributed storage. Specifically, the information owner encrypts blocks of content with distinctive and symmetrical content keys that are additional encrypted underneath a master public key. For access management, the server uses proxy cryptography to directly reencrypt the suitable content key(s) from the master public key to a granted user's public key. Sadly, a collusion attack between the untrusted server and any revoked malicious user is launched, that permits them to find out the secret writing keys of all the encrypted blocks.

In [3], Yu et al. given a climbable and fine-grained information access management theme in cloud computing supported the KP-ABE technique. The information owner uses a random key to cipher a file, wherever the random secret is more encrypted with a collection of attributes using KP-ABE. Then, the cluster manager assigns an access structure and therefore the corresponding secret key to licensed users. The access structure of every user will therefore be outlined as a novel logical expression over these attributes to replicate the scope of information files that the user is allowed to access. To enforce these access structures, we tend to outline a public key part for every attribute. Information files are encrypted mistreatment public key elements corresponding to their attributes. User secret keys are outlined to replicate their access structures so a user is ready to decode a ciphertext if and as long as the information file attributes satisfy his access structure. To attain user revocation, the manager delegates' tasks of knowledge file reencryption and user secret key update to cloud servers. However, the one owner manner could hinder the implementation of applications with the state of affairs, wherever any member during a cluster ought to be allowed to store and share information files with others.

Lu et al. [7] planned a secure provenance theme that is made upon cluster signatures and ciphertext-policy attribute-based secret writing techniques. Significantly, the system in their theme is ready with one attribute. Every user obtains 2 keys once the registration: a group signature key and an attribute key. Thus, any user is in a position to code information file mistreatment attribute-based secret writing and others within the cluster will rewrite the encrypted data mistreatment their attribute keys. Meanwhile, the user signs encrypted information along with her cluster signature key for privacy protective and traceability. However, user revocation is not supported in their theme.

From the on top of analysis, we are able to observe that the way to firmly share knowledge files in an exceedingly multiple-owner manner for dynamic and huge teams whereas conserving identity privacy from associate untrusted cloud remains to be a difficult issue. In this paper, we tend to propose a unique protocol for secure knowledge sharing in cloud computing. Compared with the present works, this theme offers distinctive features as follows:

1. Any user within the group will store and share information files with others by the cloud.
2. The secret writing quality and size of ciphertexts are freelance with the quantity of revoked users within the system.
3. User revocation will be achieved while not change the non-public keys of the remaining users.
4. A brand new user will directly decipher the files keep within the cloud before his participation.
5. The public key remains unchanged if new members are additional to the group. The schemes even conceal the scale of the group.
6. The lengths of the general public key and of the signatures are, similarly because the procedure effort for signing and verifying, freelance of the quantity of group members.
7. Group Manager cannot pretend the signature by exploitation blinded public key.

III. PRELIMINARIES

a. Bilinear Maps

Let G1 and G2 be an additive cyclic group and a multiplicative cyclic group of the same prime order q, respectively [11]. Let e: G1 × G1 →G2 denote a bilinear map constructed with the following properties:

1. Bilinear: For all a, b € Z^*_q and P, Q € G1, $e(aP, bQ) = e(P,Q)^{ab}$.
2. Nondegenerate: There exists a point P such that $e(P, P) \neq 1$.
3. Computable: There is an efficient algorithm to compute e(P, Q) for any P, Q € G1.

b. Complexity Assumptions

Definition1: (q-strong Diffie-Hellman (q-SDH) Assumption [12]). Given (P1, P2, YP2, Y2P2. YqP2), it is infeasible to compute $\frac{1}{Y+\times}$ P1, where ×€ Z^{*}_{q}

Definition 2 (Decision linear (DL) Assumption [12]). Given P1, P2, P3, aP1, bP2, cP3, it is infeasible to decide whether a + b = c mod q.

Definition 3 (Weak Bilinear Diffie-Hellman Exponent (WBDHE) Assumption [13]). For unknown a€ Z^{*}_{q}, given Y, aY,a^2Y…a^lY,P€G1, it is infeasible to compute e(Y,P)$\frac{1}{a}$

Definition 4 ((t, n)-general Diffie-Hellman Exponent (GDHE) Assumption [14]). Let $f(x) = \prod_{i=1}^{n-1} X + x'i$be the two random univariate polynomials. For unknown k, □€ Z^{*}_{q}, givenG0,□G0,…,$□^{t-1}$G0,□f(□)G0,P0,…,$□^{t-1}$P0,kg(□)H0 €G1 and $e(G0,H0)^{f2(□)g(□)}$€ G2; it is infeasible to compute $e(G0,H0)^{kf(□)g(□)}$€ G2.

c. Group Signature

A new kind of signature for a group of persons, referred to as a group signature that has the subsequent properties.

- Only member of the group will sign messages.
- The receiver will verify that it is a legitimate group signature, however cannot discover that group member created it.
- If necessary, the signature is "opened", in order that the one that signed the message is discovered.

d. First Efficient Group Signature Scheme

Group Signature have the subsequent undesirable properties:

- The length of the group's public key and/or the size of a signature depend on the size of the group. This can be terribly problematic for large groups.
- To add new group members, it is necessary to switch a minimum of the general public key.

In this paper, the first efficient group signature schemes that overcome these issues. The lengths of the general public key and of the signatures are, as well as the computational effort for signing and validatory, freelance of the amount of group members. Moreover, the general public key remains unchanged if new members are added to the group. The schemes even conceal the dimensions of the group.

e. Blinded Public key

Group Manager is aware of all the secret keys of the group members and may so additionally produce signatures. This could be prevented by victimization blind public keys. Let the general public key system used be supported. Let g be a generator of the multiplicative cluster Z^{*}_{p} wherever p could be a prime. Cluster member i creates his own secret key s_i and provides g^{si} (mod p) to Manager. Therefore Manager encompasses a list of these publickeys alongside the group member's name. Each week Manager provides every group member i a randomly chosen range r_i€ (1... p- 1) and publishes the list of all the blind public keys $(g^{si})^{ri}$. Throughout in the week group member i will use $s_i r_i$ (mod p - 1) as secret key. The benefits of this modification are that manager cannot pretend signatures, which every group member only needs to have one "really secret key" (for instance during a sensible card), which may be blind so as to create different secret keys. Solely the one week's signatures may be connected, so every group member will have solely a number of secret keys in his smart card to stop this linking. If an r_i is accidentally disclosed, still no additional data concerning the secret key s_i is disclosed.

f. Broadcast Encryption

Broadcast encryption is a noteworthy application of cryptography that permits one to broadcast a secret to a ever-changing group of intended recipients in such the way that nobody outside this group will read the secret. A broadcasting theme involves encrypting a message so quite one privileged receiver will decode it. To attain that, privileged receivers are classified along either dynamically or statically in keeping with the theme getting used. Two totally different broadcast cryptography techniques are described in this section. One in every of these themes could be a stateful theme and therefore the different one could be a stateless scheme.

Stateful schemes

A stateful broadcast encoding theme needs that everyone the receivers need to be able to update the stored keys, typically once receivers are added or faraway from the privileged receiver set Rp. This means that any receiver r €Rp should be connected all the time to the published network Q so as to not lose any key update message which may be sent.

Stateless schemes

A stateless broadcast encoding theme means all receivers cannot update their keys between sessions, that is, the data formatting step is performed just one occasion and when the data formatting step all receivers have the information that is required to rewrite future broadcast message. An example on wherever a stateless broadcast encoding theme is employed is pay TV shows. Once a brand new user subscribes to a pay television show, then the user receives a smartcard that contains the coding key and may be used for decrypting the published.

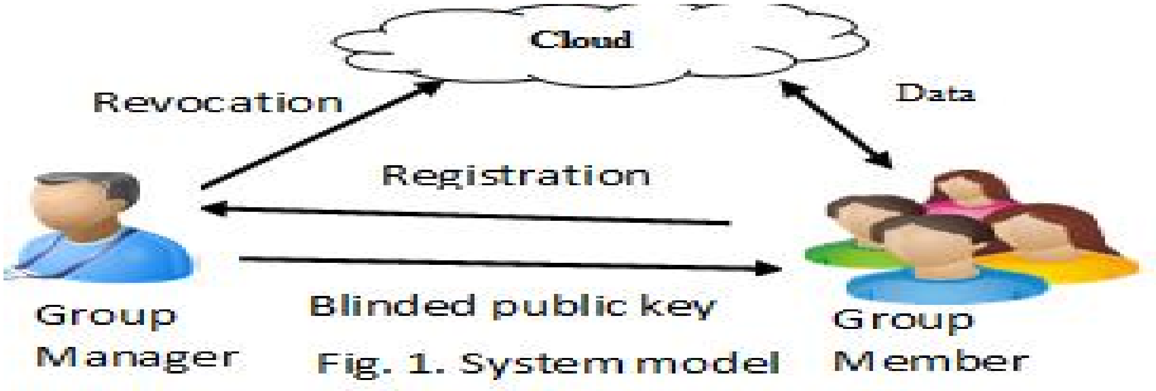

Fig. 1. System model

IV. SYSTEM MODEL

A cloud computing design by combining with an example that a corporation uses a cloud to alter its staffs within the same group or department to share files. The system model consists of 3 totally different entities: the cloud, a group manager (i.e., the corporate manager), and an oversized range of group members (i.e., the staffs) as illustrated in Fig. 1. System model.

Cloud is operated by CSPs and provides priced thick storage services. However, the cloud is not absolutely trustworthy by users since the CSPs are terribly possible to be outside of the cloud users' trustworthy domain. Just like [3], [7], we tend to assume that the cloud server is honest however curious. That is, the cloud server won't maliciously delete or modify user information due to the protection of information auditing schemes, however can try and learn the content of the keep information and therefore the identities of cloud users.

Group manager takes charge of user registration, user revocation, system parameters generation and revealing the identity of a dispute information owner. Within the given example, the group manager is acted by the administrator of the corporate. Therefore, we tend to assume that the group manager is absolutely trustworthy by the opposite parties.

Group members are a set of registered users which will store their personal information into the cloud server and share them with others within the group. In our example, the staffs play the role of group members. Note that, the group membership is keep on modified, as a result of the employees' resignation and new worker participation within the company**.**

V. CONCLUSION

In this paper, we have a tendency to tend to style a secure data sharing theme, for dynamic and large groups in associate degree untrusted cloud. A user is during a position to share data with others at intervals the cluster whereas not revealing identity privacy to the cloud. Additionally, it supports economical user revocation and new user connexion. Plenty of specially, economical user revocation is also achieved through a public revocation list whereas not change the personal keys of the remaining users, and new users can directly rewrite files keep at intervals the cloud before their participation.

The overall public key remains unchanged if new members square measure any to the cluster. The schemes even conceal the scale of the cluster. The lengths of the ultimate public key and of the signatures are, equally as a results of the procedure effort for sign language and verifying, freelance of the number of group members. Moreover, the storage overhead and conjointly the secret writing computation worth are reduced. Thorough analyses show that planned theme satisfies the desired security needs and guarantees efficiency what is more.

VI. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracings Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[13] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.