JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Survey on User Group Revocation and Integrity Auditing of Shared Data in Cloud Environment

Rohit Rai[1*], **Upasna Singh**[2]

[1]Department of Computer Science & Engineering, Defence Institute of Advance Technology, Pune, India
[2]Department of Computer Science & Engineering, Defence Institute of Advance Technology, Pune, India

[*]Corresponding Author: rohit.elextron@gmail.com, upasna.diat@gmail.com

Available online at: www.ijcseonline.org

Accepted: 06/Dec/2018, Published: 31/Dec/2018

Abstract— The term 'group Signature' is inherited element of 'digital signature' that permits any group members to sign the messages on behalf of its group which they belongs too. The identity of original signer is hidden by this resulting signature. Subsequently, the identity of the original signer can be reveal by the group manager, who is only responsible to, open the signatures respectively. The efficient approach that combines the revocation mechanism into group signature schemes based on the robust RSA assumption. The security is an essential factor for a secure group signature scheme, and the third party introduction make the scheme more practical and simple than the previous schemes of this kind.

Keywords— Group signature scheme, Cloud computing, Revocation, RSA Algorithm.

I. INTRODUCTION

A member at an institution would want to share their findings & observations with their team members. Ideally, members on the same team should be able to access all of the desired information. This would requisite storage of information at a Local facility. However, this may lead to furthering of difficulty of information sharing as the site would require maintenance and security. Outsourcing of data or time-consuming computational workloads on the cloud solves the problems of maintenance, reduces the needless repetition of data information, which decrease the burden on individuals or enterprises/institutions [1].

While there are benefits of shifting to cloud, it also brings with itself unreliability. The outsourced data are susceptible to being leaked and tampered with. In Third Party cloud services (TPCs), users generally have very little control over how their data is handled by the cloud and therefore difficult to guarantee security of the stored data.

Additionally, there are cases in which a user would prefer to anonymously achieve data sharing in the cloud. It is particularly an important feature for whistleblowers to highlight illegal and unethical cases within a group/organization without revealing its identity. There are also cases, when a user may misuse this anonymity. To prevent such cases, it should be possible to arrive at the user identity, through some means, if so desired.

Sometimes, a user wants to verify whether the data she wants to access is the same data that was initially uploaded on the cloud. For this, a Scheme needs to be publicly verifiable. A Publicly Verifiable Scheme is one in which there is a provision for the data user to confirm the integrity of the stored data through an established mechanism like third party auditor.
Therefore, The purpose of the contribution to achieve dynamic data sharing between a group under a cloud computing environment anonymously, with provision for Public Integrity auditing and group User revocation [3].

The remaining part of this paper is organized as follows: Section I contains the introduction of "User Group Revocation and Integrity Auditing of Shared Data in Cloud Environment" Section II discuss about some key challenges that are faced during secure data sharing. Section III reviews some of the existing works related to public integrity auditing in cloud. Section IV presents the detailed description for the key components of cloud integrity auditing system. Section V presents the literature survey of different papers. Finally, this paper is concluded to be carried out is stated in Section VI.

II. CHALLENGES FACED

The achievement of the aforementioned goals would merit consideration of the following challenges:-

(a) Firstly, the scheme should be able to support variable number of group members. In real life scenarios the number of members in each group is arbitrary; members join and exit the group dynamically and regularly. Therefore, a desired scheme should be able to supports the inclusion of any number of users. It should also be able to provide for data and key updating. Once data are outsourced to the cloud, it will not remain unchanged for the entire period it is on the cloud. In other words, a data owner might demand to update (insert, delete, or modify) their cloud data. So, dynamic support for cloud data is of great necessity [10].

(b) Secondly, the confidentiality of the outsourced data should be preserved. Since the uploaded data may be sensitive and confidential business plans or scientific research achievements, data leakages may cause significant losses or serious consequences [10]. Without the guarantee of confidentiality, users would not like to be involved in the cloud to share data. To achieve the confidentiality of the Message (Mx), the client can use his/her secret key to encrypt each Mx using an encryption scheme. When there is only one user (data owner) in the group, the user only needs to choose a random secret key and encrypt the data using a secure symmetric encryption scheme. However, when the scheme needs the support multi-user data modification, while at the same time keeping the shared data encrypted, a shared secret key among group users will result in single point failure problem. It means that any group user can leak the shared secret key will break the confidentiality guarantee of the data [13].

(c) Thirdly, any user in the group should be provisioned, in an unrestricted manner, to store and read their data stored in the cloud, and the deletion of data is performed by the user. It is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud [11, 12].

(d) Finally, there should be a provision to trace back the user in case he behaves inappropriately. A badly behaved user may Therefore, it is necessary to provision for authentication. In the many-to-many group data sharing pattern, it is essential to provide authentication services to resist misbehaving users. For instance, a misbehaving user may intentionally upload incorrect data or ambiguous data to disrupt the cloud storage system.

(e) Public Integrity auditing: A scheme should support public integrity auditing. A publicly verifiable Scheme allows the data integrity check to be performed not only by data owners, but also by any third-party auditor [13].

III. EXISTING SYSTEM

For providing the data privacy, integrity and availability of traditional cloud store, existing systems provides some solutions. In these solutions, when a scheme helps data modification, then that is a dynamic scheme. This scheme is openly verifiable it means that data integrity check can be performed not only by data owners, but also by any third-party auditor. However, the dynamic schemes focus on some cases where there is a data owner and only the data owner could modify the data. The user revocation problem is not examined and the auditing cost is linear to the group size and data size. Wang et al. proposed data integrity based on ring signature to support multiple user data operations. To improve the previous scheme and make it more efficient and scalable, Yuan and Yu has designed a dynamic public integrity auditing scheme with group user revocation. [1, 2]

DISADVANTAGES OF EXISTING SYSTEM

- In this scheme of Wang et al., the auditing cost is linear to the group size and data size and the user revocation problem is not considered.
- However, in Yuan and Yu scheme, the authors do not consider the data secrecy of group users that is their scheme could efficiently support plaintext data update and integrity auditing, while not cipher text data.
- The cloud itself could conduct the user revocation phase that is the data owner does not take part in the user revocation phase.

IV. KEY COMPONENTS DETAIL DESCRIPTION

A. Public Integrity Auditing

The drawbacks of existing system motivated to explore more about how to design a reliable and efficient scheme, while achieving secure group user revocation. The new idea called Public Integrity Auditing for shared dynamic cloud data with group user revocation explores how to design an efficient and reliable scheme. It not only keeps group data encryption and decryption during the data modification processing, but also realizes efficient and secure user revocation [3].

The investigation on the efficient and secure shared data incorporates auditing for multi-user operation for cipher text database. An efficient data auditing scheme provide some new features, such as traceability and countability. [6]

The enhancements and improvements in cloud computing motivates organization and enterprises to outsource their data to third party cloud service providers (CSP's) which will result in improvements in the data storage limitation of resource constrained local devices.

1. DATA OWNER: Data owner is responsible for view and upload file on the cloud. Data owner must have to register in the system. [7]

2. DATA USER: Data user is the one who is responsible for view files uploaded by data owners and download that files. To download file from cloud data user has to be authenticated user otherwise he will be considered as attacker. [7]

3. THIRD PARTY AUDITOR (TPA): Third party auditor is an authorized person. TPA has rights to validate authorized data owner as well as the user. TPA is also responsible for allocation of block and maintains information as well as authentication. [7]

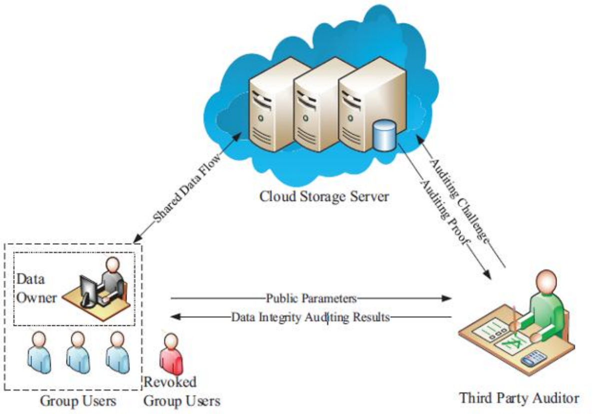

Figure: Public Integrity Auditing

4. CLOUD STORAGE SERVER: Cloud storage server holds data or files of the data owner on the cloud. data owner have to pay charges for it. [7]

B. *Data Group sharing:*

There is multiple numbers of users who registered and stores their private data into cloud server and also share them with others in the group. While sharing the data into cloud no one can directly access that file till he or she have group signature key to access shared file. Once he or she gets the key then they can access file which is shared by data owner respectively. [6]

C. *Group signature:*

The Group signature schemes are a main building block for many security applications. A group signature scheme includes both a group manager and group members. The group manager owns group master keys while each member holds its group member key, or group member certificate. Enabling data sharing and storage for the same group in the cloud with high security and efficiency in an anonymous manner. [9]

By leveraging the key agreement and the group signature, a traceable group data sharing scheme can be proposed to support anonymous multiple users in public clouds. On the one hand, group members can communicate anonymously with respect to the group signature, and the real identities of members can be traced if necessary.

On the other hand, a common conference key is derived based on the key agreement to enable group members to share and store their data securely. There are different ways in which common conference key can be generated. The traditional techniques mostly utilize Asymmetric key cryptography techniques. However, of late block designs are also utilized for key generation, which substantially reduces the burden on members to derive a common conference key.
In a Group signature scheme, there are three major components. The same is postulated below: [9]

(i) Group Manager: The manager of group for managing the memberships and generating the membership keys of group members (Signers). Group Manager, revealing the identity of the signature's originator when dispute.

(ii) Group Member: The group member, he/she have his/her membership key, and he/she can using the membership key to sign message on behalf of the group which they belong.

(iii) Verifier: Receiver of group signature can check the validity of the group signature by the group members.

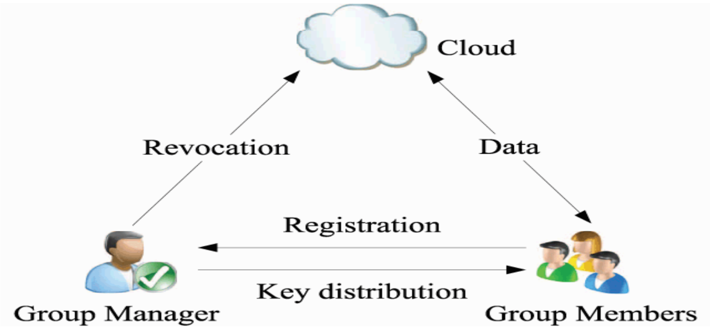

Figure:Layout of standard group signature.

The scheme consists of some important protocols: [9]

a. KeyGen: The group manager uses KeyGen protocol to generate masterkey and its system parameters.

b. Join: The group manager runs join protocol, together to obtain a certificate to represent its group membership.

c. Sign: A group member anonymously sign a message following sign protocol.

d. Open: The group manager uses open protocol to find the signer of a signature.

e. Revoke: the group manager uses revoke protocol to exclude a group member.

D. Requirements of group signature:

A secure group signature scheme must satisfy the following basic requirements [6, 20]:

a. Unforgeability: Only group members can issue valid signatures on behalf of the entire group.

b. Conditional Signer Anonymity: Anyone can easily check that a message /signature pair was signed by some group member, but only the group manager can determine which member issued the signature.

c. Undeniable Signer Identity: The group manager can always determine the identity of the group member who issued a valid signature.

d. Unlinkability: Determining if two different signatures were computed by the same group member is computationally infeasible for everyone but the group manager.

e. Security against Framing Attacks: No subset of group members can sign a message on behalf of another group member. That is, if the Open procedure is invoked on the message, it should not specify the name of another group member not belonging to the original subset.

f. Traceability: A trusted entity can always open a valid signature using the OPEN procedure and identify the actual signer.

g. Revocability: The group manager can revoke a group member so that this group member cannot produce a valid group signature any more after being revoked.

h. Unforgeable tracing verification: The revocation manager cannot falsely accuse a signer of creating a signature he did not create

i. Distinguishable: Due to different member group signature keys are different and each group private key is unique, so we can distinguish group members according to their corresponding private keys.

j. Non-repudiation: Once a member makes his signature, the synthesis mapping T will contain his private key. Each group private key is unique and only the members have their own private keys. Therefore, no one can dismiss the signature once he made the signature.

k. Countability. A scheme is countable, if for any data the TPA can provide a proof for this misbehaviour, when the dishonest cloud storage server has tampered with the database.

E. ALGORITHM DETAILS

1. RSA Algorithm

RSA is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private Key is kept private.

For Example: - Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key.[18]

Table1: RSA Algorithm

Step 1	Choose two distinct prime numbers p and q. ● For security purposes, the integer's p and q should be chosen at random, and should be similar in magnitude but 'differ in length by a few digits to make factoring harder. Prime integers can be efficiently found using a primality test.
Step 2	Compute $n = pq$. ● n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
Step 3	Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function. This value is kept private.
Step 4	Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
Step 5	Determine d as $d \equiv e^{-1}$ (mod $\varphi(n)$); i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$) ● This is more clearly stated as: solve for d given $d{\cdot}e \equiv 1$ (mod $\varphi(n)$) ● e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65,537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings. ● e is released as the public key exponent. ● d is kept as the private key exponent.

	The *public key* consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

2. *AES Algorithm*

The Advanced Encryption Standard (AES) algorithm is one of the block cipher encryption algorithm. This is used for encryption and decryption of text. AES works by repeating the same defined steps multiple times. [19]

Table2: AES Algorithm

Step 1	**a. Encryption** You take the following AES steps of encryption for a 128-bit block: 1. Derive the set of round keys from the cipher key. 2. Initialize the state array with the block data (plaintext). 3. Add the initial round key to the starting state array. 4. Perform nine rounds of state manipulation. 5. Perform the tenth and final round of state manipulation. 6. Copy the final state array out as the encrypted data (cipher text).
	Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called: 1. Sub-Bytes 2. Shift-Rows 3. Mix-Columns 4. Xor-Round Key
Step 2	**b. Decryption** As you might expect, decryption involves reversing all the steps taken in encryption using inverse functions: 1. InvSub-Bytes 2. InvShift-Rows 3. InvMix-Columns Operation in decryption is: **1. Perform initial decryption round:** ● Xor-Round Key ● InvShift-Rows ● InvSub-Bytes **2. Perform nine full decryption rounds:** Xor-Round Key InvMix-Columns InvShift-Rows InvSub-Bytes **3. Perform final Xor-Round Key:**

V. Related Work

J. Yuan and S. Yu, [1] presented efficient public integrity checking for cloud data sharing with multi-user modification in which is featured by salient properties of public integrity checking and continual computational cost on user side. This through our novel design on polynomial based authentication tags which allow accumulation of tags of different data blocks.

B. Wang, L. Baochun, and L. Hui, [2] presented public auditing for shared data with efficient user revocation in the cloud. By utilizing the idea of proxy re-signatures, they allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud.

Ashwin S. Bande and S. G. Shikalpure [3] has proposed for dividing task into the three entities, Group Manager, Opening Manager and Revocation Manager, to increase the privacy of the user by dividing the work of the group manager into three entities. Group Manager can only create group and add members in group but does not possesses power to open any signature. The Open Manager possesses a special key which can be used only to open a signed message. The Revocation Manager, who can only get secret key of a member from Open Manager's request, can revoke that member but cannot revoke any other member whose secret key is not known to him

Rupeng Li, Jia Yu, Jin Wang,Guowen Li, Daxing Li [4] In proposed scheme to overcome the problem of key damage, in which the key is stored on the physical device they implemented VLR and random access key update scheme. Where they try to solve the problem of key exposure in group signature schemes and proposed the notion of key insulated group signature with VLR.

Shi Cui and Xiangguo Cheng [5] The main idea behind our scheme is that the secret key of the group is split into two parts by GM, one part is given to the user as his group membership secret key, and the other is given to SEM. Neither the group member nor SEM can sign a message without the other's help. To revoke the membership of a group member, GM need only ask SEM not to provide the group member partial signatures any more.

C. Wang, Q. Wang, K. Ren, and W. Lou,[6] presented privacy-preserving public auditing for data storage security in cloud computing utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.

Subhra Mishra and Tilak Rajan Sahoo[7] The scheme implemented by us provides these features. The use of elliptic curve cryptography increases the security the scheme by providing desired security level that is achieved by significantly smaller keys in elliptic curve system than in its counterpart- RSA system. Another significant advantage being in general, the algorithms used for encryption and decryption in ECC schemes are faster and can be run on machines that are less efficient.

Pushkar Zagade, Shruti Yadav , Aishwarya Shah, Ravindra Bachate [8] In this paper there will be auditing the integrity of shared data with dynamic groups in cloud. A new user can be added into the group and an existing group member can be revoked by preserving privacy including data backup based on vector commitment and verifier-local revocation group signature. This scheme supports the public validation and efficient user revocation and also some nice properties such as traceability, efficiency, confidently, countability. Finally, the security and experimental analysis show that our scheme is also secure and efficient.

X. Liu, Y. Zhang, B. Wang, and J. Yan, [11] combines the group signature and dynamic broadcast encryption techniques. The group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users. The group manager computes the revocation parameters and makes the result publically available by migrating them into the cloud. Thus, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation.

T. Jiang, X. Chen and J. Ma [13]. Proposes two entities in their model. (a) Group users which consist of a data owner & a number of users who are authorized to access and modify the data by the data owner. And Data Owner is supported to securely revoke the users which are founded as malicious in group. (b) TPA (Third Party auditor) which is the entity in the cloud server which will be able to conduct the data integrity check of the shared data on the server. This paper proposes the public integrity auditing for shared dynamic cloud data with group user revocation scheme using Asymmetric group key agreement scheme (ASGKA). In ASGKA, all the users arrive at a common shared encryption key. It is formed by tensor product of individual public keys generated by various users. Also, in this scheme, the public key can be simultaneously used to verify signatures and encrypt messages while any signature can be used to decrypt cipher text under this public key.

Dan Boneh and Hovav Shacham [14] has proposed three algorithms for verifier local revocation:

(a) KeyGen(n): This randomized algorithm takes as input a parameter n (the number of members of the group). It outputs: a group public key (gpk) ,an n-element vector of user keys gsk [1] gsk[2]; gsk[i]; . . . ; gsk[n], and an n-element vector of user revocation tokens grt, similarly indexed.

(b) Sign (gpk,gsk[i],M): This randomized algorithm takes as input the group public key gpk, a private key gsk[i],and a message M, and returns a signature s.

(c) Verify (gpk, RL, s, M): The verification algorithm takes as input the group public key gpk, a set of revocation tokens RL (whose elements form a subset of the elements of grt), and a claimed signature s on a message M. It returns either valid or invalid. The latter response can mean either that s is not a valid signature, or that the user who generated it has been revoked.

S. Cui, X. Cheng and C. W. Chan,[15] proposed that the secret key of the group is split into two parts by GM, one part is given to the user as his group membership secret key, and the other is given to SEM. Neither the group member nor SEM can sign a message without the other's help. To revoke the membership of a group member, GM need only ask SEM not to provide the group member partial signatures any more.

R. Li, J. Yu, J. Wang, G. Li and D. Li, [16] proposed that, to overcome the problem of key damage, in which the key is stored on the physical device, they implemented VLR and random access key update scheme, where they try to solve the problem of key exposure in group signature schemes and proposed the notion of key insulated group signature with VLR.

VI. CONCLUSION

The result of the survey provides some eventful way to solve the problem of verifiable outsourcing of storage by introducing verifiable database with efficient updates. It also clears up efficient and secure data integrity auditing to share dynamic data with multiuser modification. The public data auditing, enable outsource cipher text database to remote cloud and support secure group users revocation to shared dynamic data. The main focus is on data sharing and its storage for the same group in the cloud with high security and efficiency in an anonymous manner. The prospect for efficient and secure data integrity auditing is by using group user revocation for shared dynamic cloud data. We have also explored the RSA and AES algorithms that are used for security purpose.

ACKNOWLEDGMENT

The authors would like to thank the publishers and researchers for making their resources available. We also thank the college authority for providing the required infrastructure and support.

REFERENCES

[1] J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. of IEEE INFOCOM 2014, Toronto, Canada, Apr. 2014, pp. 2121–2129.

[2] B. Wang, L. Baochun, and L. Hui, "Public auditing for shared data with efficient user revocation in the cloud," in Proc. Of IEEE INFOCOM 2013, Turin, Italy, Apr. 2013, pp. 2904–2912.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preservingpublic auditing for data storage security in cloud computing,"inProc. of IEEE INFOCOM 2010, CA, USA, Mar. 2010, pp. 525–533.

[4] Pushkar Zagade, Shruti Yadav, Aishwarya Shah, Ravindra Bachate " Group User Revocation and Integrity Auditing of Shared Data in Cloud Environment" *International Journal of Computer Applications (0975 – 8887) Volume 128 – No.12, October 2015.*

[5] Subhra Mishra and Tilak Rajan Sahoo" A Survey on Group Signature Schemes" Department of Computer Science and Engineering National Institute of Technology Rourkela Rourkela.

[6] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma" Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation" 2015 IEEE.

[7] He Ge "An Effective Method to Implement Group Signature with Revocation".

[8] Rupeng Li, Jia Yu, Jin Wang,Guowen Li, Daxing Li" Key-Insulated Group Signature Scheme with Verifier-Local Revocation" 2007 IEEE.

[9] Aayush Agarwal, Rekha Saraswat "A Survey of Group Signature Technique, its Applications and Attacks" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 10, April 2013.

[10] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

[11] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib.Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. Conf. Inf. Commun., 2010, pp. 1–9.

[13] T. Jiang, X. Chen and J. Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation," in IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363-2373, 1 Aug. 2016.

[14] Dan Boneh and Hovav Shacham. 2004. Group signatures with verifier-local revocation. In Proceedings of the 11th ACM conference on Computer and communications security (CCS '04). ACM, New York, NY, USA, 168-177.

[15] S. Cui, X. Cheng and C. W. Chan, "Practical group signatures from RSA," *20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06)*, Vienna, 2006

[16] R. Li, J. Yu, J. Wang, G. Li and D. Li, "Key-Insulated Group Signature Scheme with Verifier-Local Revocation," *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, Qingdao, 2007

[17] X. Yi, "Identity-based fault-tolerant conference key agreement," IEEE Trans. Depend. Sec. Comput., vol. 1, no. 3, pp. 170–178, Jul. 2004.

[18] Evgeny Milanov "The RSA Algorithm" published on 3 June 2009

[19] Ako Muhamad Abdullah "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data" 16 June 2017.

[20] Mr. Mangesh Nagarkar , Prof. Patole R.G "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation" International Journal of Advanced Research in Computer and Communication Engineering. Vol. 5, Issue 11, November 2016.

Authors Profile

Rohit Rai completed his Bachelor of Technology from North Eastern Regional Institute of Science and Technology, India in 2009. Currently, he is Pursuing M.Tech in Computer Science & engineering from Defence Institute of Advance Technology, Pune, India. He is working on the project **"Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation".** His interest areas are Cryptography and Network Security, Operating Systems.

Upasna Singh is a Assistant Professor at Defence Institute of Advance Technology, Pune, India. Her Research areas include Digital Forensics, Social Network Analysis, Data Mining & Knowledge Discivery and Soft Computing. She is a member of Computer Society of India & Indian Society for Rough Sets. She has more then 15 publications to her name.