Authentic and Anonymous Data Sharing with Enhanced Key Security

Dhanshree Sanjay Madnaik[1], Suhas B. Bhagate[2]

[1]Student, Dept. of Computer Science and Engineering, D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji, Maharashtra, India
[2]Professor, Dept. of Computer Science and Engineering, D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji, Maharashtra, India

Abstract – *Data sharing has never been less demanding with the advances of cloud computing, mutual data gives a variety of advantages to both the general public and people. Data sharing with countless must consider a few issues, including proficiency, data uprightness and security of data proprietor. Ring signature is a promising possibility to build an unknown and real data sharing framework. It permits a third party auditor to secretly validate his data which can be put into the cloud for capacity or examination reason. Yet the immoderate authentication confirmation in the customary public key infrastructure (PKI) setting turns into a bottleneck for this answer for be versatile. Character based (ID-based) ring signature, which takes out the procedure of declaration check, can be utilized. We further upgrade the security of ID-based providing so as to ring signature forward security: If a mystery key of any client has been traded off, all past produced signatures that incorporate this client still remain substantial. This property is particularly critical to any substantial scale data sharing framework, as it is difficult to ask all data proprietors to re-authenticate their data regardless of the fact that a mystery key of one single client has been traded off. So for that purpose we proposed third party auditor to evaluate and uncover risk of cloud storage services on benefit of the client's request. We give a solid and productive instantiation of our plan, demonstrate its security and give an execution to demonstrate its reasonableness.*

Key Words: Public key certificates, Digital signature, Encryption-Decryption, ID-based Ring signature, AES Algorithm.

1. INTRODUCTION

The prevalence and across the board utilization of "CLOUD" have brought extraordinary comfort for data sharing and accumulation [1], [2]. Not just can people obtain valuable data all the more effectively, sharing data with others can give various advantages to our general public too. As a delegate illustration, purchasers in Smart Grid can get their vitality use data in a fine-grained way and are empowered to impart their own vitality use data to others, e.g., by transferring the data to an outsider stage such as Microsoft Home. From the gathered data a factual report is made, and one can think about their vitality utilization with others. This capacity to get to, break down, and react to a great deal more exact and itemized data from all levels of the electric lattice is basic to effective vitality utilization. Because of its openness, data sharing is constantly conveyed in a threatening situation and defenceless against a number of security dangers. To solve this problem we proposed third party auditor to evaluate and uncover risk of cloud storage services on benefit of the client request. Data sharing is always deployed in a hostile environment and vulnerable to a number of security threats. ID-based cryptography was introduced by Shamir [3] as a solution to the difficulty and complexity of public key certificate management in conventional public key cryptography, this scheme has limitations because of a trusted key for secret key generation and use of secure channels for secret key distribution.

In the enhance key security there are four phases which are used for the security of ring user setup phase, key generation phase, signing of keys and verification of keys phase. The set up phase includes choosing randomly master secrete key and computing corresponding public key. The signer with the identity sets the public key and computes the signer's private key. It sends the private signing key to the signer via a secure channel. For the signing with key for group of identifiers having each user identity, the computation of keys common to all ring members is calculated. A verifier can check the validity of a signature for the message m and a set of identifiers. Authentication is the act of confirming the truth of an attribute of a single piece of data or entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artefact by carbon dating, or ensuring that a product is what its packaging and labelling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

Identity-based Ring Signature private or hybrid Identity-based (ID-based) cryptosystem, introduced by Shamir, eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming. In an ID based cryptosystem, the public key of each user is easily computable from a string corresponding to this user's publicly known identity (e.g., an email address, a residential address, etc.). A private key generator (PKG) then computes private keys from its master secret for users.

This property avoids the need of certificates (which are necessary in traditional public-key infrastructure) and associates an implicit public key (user identity) to each user within the system. In order to verify an ID-based signature, different from the traditional public key based signature, one does not need to verify the certificate first. The elimination of the certificate validation makes the whole verification process more efficient, which will lead to a significant save in communication and computation when a large number of users are involved. Enhanced security is same as the forward secrecy. In forward secrecy a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. Even worse, the “group" can be defined by the adversary at will due to the spontaneity property of ring signature: The adversary only needs to include the compromised user in the “group" of his choice. As a result, the exposure of one user’s secret key renders all previously obtained ring signatures invalid if that user is one of the ring members, since one cannot distinguish whether a ring signature is generated prior to the key exposure or by which user. Therefore, enhanced key security is a necessary requirement that a big data sharing system must meet. Otherwise, it will lead to a huge waste of time and resource. In the traditional public key setting where signature verification involves expensive certificate check for every ring member. This is far below satisfactory if the size of the ring is huge, such as the users of a Smart Grid. Third Party Auditor is a substance, which has expertise and capabilities that customers don't have, is trusted to evaluate and uncover risk of cloud storage services on benefit of the customers upon request.

1.1 Need of Work

To verify an ID-based ring signature, only the identities of ring users, together with the pair of message and signature are needed. The elimination of certificate validation is a difficult process, saves a great amount of time and computation. This saving will be more critical if a higher level of anonymity is needed by increasing the number of users in the ring. The ring signature improves the privacy preserving capability of group signatures by removing the need for a group manager and by allowing a signer to create an ad-hoc group membership even without or less knowledge of the other members. The ring signature scheme is an excellent way for use in applications with the competing requirements of message authenticity and signer privacy.

ID-based ring signature is more advantageous and preferred in the setting with a large number of users. Costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck. Identity-based (ID-based) ring signature, eliminates the process of certificate verification and third party auditor which evaluate and uncover risk of cloud storage services.

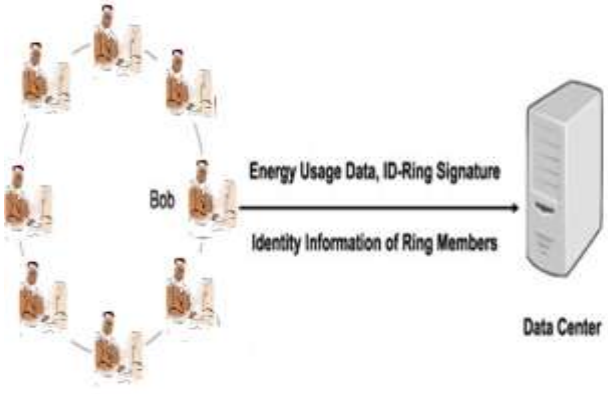
Bob
Energy Usage Data, ID-Ring Signature
Identity Information of Ring Members
Data Center

Fig.1.1 ID based ring signature

Suppose there are 10,000 users in the ring, the verifier of a traditional public key based ring signature must first validate 10,000 certificates of the corresponding users, after which one can carry out the actual verification on the message and signature pair. In contrast, to verify an ID-based ring signature, only the identities of ring users, together with the pair of message and signature are needed. As one can see, the elimination of certificate validation, which is a costly process, saves a great amount of time and computation. This saving will be more critical if a higher level of anonymity is needed by increasing the number of users in the ring. Thus, as depicted in Fig. 1, ID-based ring signature is more preferable in the setting with a large number of users such as energy data sharing in smart grid

2. Methodology

The proposed system will be designed and implemented in the following modules,

Authentication is the act of confirming the truth of an attribute of a single piece of data or entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artefact by carbon dating, or ensuring that a product is what its packaging and labelling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

Data sharing is the practice of making data used for scholarly research available to other investigators. Replication has a long history in science. A number of funding agencies and science journals require authors of peer-reviewed papers to share any supplemental information (raw data, statistical methods or source code) necessary to understand, develop or reproduce published research. A great deal of scientific research is not subject to data sharing requirements, and many of these policies have liberal exceptions. In the absence of any binding requirement, data sharing is at the discretion of the scientists themselves. In addition, in certain situations agencies and institutions prohibit or severely limit data sharing to protect proprietary interests, national security, and subject/patient/victim confidentiality. Data sharing may also be restricted to protect institutions and scientists from use of data for political purposes.

Identity-based Ring Signature private or hybrid Identity-based (ID-based) cryptosystem, introduced by Shamir, eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming. In an ID based cryptosystem, the public key of each user is easily computable from a string corresponding to this user's publicly known identity (e.g., an email address, a residential address, etc.). A private key generator (PKG) then computes private keys from its master secret for users. This property avoids the need of certificates (which are necessary in traditional public-key infrastructure) and associates an implicit public key (user identity) to each user within the system. In order to verify an ID-based signature, different from the traditional public key based signature, one does not need to verify the certificate first. The elimination of the certificate validation makes the whole verification process more efficient, which will lead to a significant save in communication and computation when a large number of users are involved.

Enhanced security is same as the forward secrecy. In forward secrecy a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. Even worse, the "group" can be defined by the adversary at will due to the spontaneity property of ring signature: The adversary only needs to include the compromised user in the "group" of his choice. As a result, the exposure of one user's secret key renders all previously obtained ring signatures invalid if that user is one of the ring members, since one cannot distinguish whether a ring signature is generated prior to the key exposure or by which user. Therefore, enhanced key security is a necessary requirement that a big data sharing system must meet. Otherwise, it will lead to a huge waste of time and resource. While there are various designs of forward-secure digital signatures adding forward security on ring signatures turns out to be difficult. There are only two forward secure ring signature schemes. However, they are both in the traditional public key setting where signature verification involves expensive certificate check for every ring member. This is far below satisfactory if the size of the ring is huge, such as the users of a Smart Grid.

Third Party Auditor is a substance, which has expertise and capabilities that customers don't have, is trusted to evaluate and uncover risk of cloud storage services on benefit of the customers upon request.

Table -1: Time for Service provider to verify ring signature

	T=100	T=200	T=300	T=400
n=10	421	452	468	484
n=20	811	827	843	889
n=30	1170	1217	1217	1248
n =40	1560	1576	1591	1622
n=50	1934	1965	2013	2043
n=60	2340	2372	2387	2401
n=70	2698	2683	2699	2730
n=80	3042	3089	3151	3167
n=90	3416	3448	3526	3541
n=100	3869	3885	3915	3935

The average time for the service provider to verify the ring signature with different choices of n and T are as shown in following figure 6.2.2 and Table 4 for |N|=1024 bits. The testbed for the user is a laptop personal computer equipped with 2.50 GHz Intel CPU with 4 GB RAM and running windows 7 operating system.

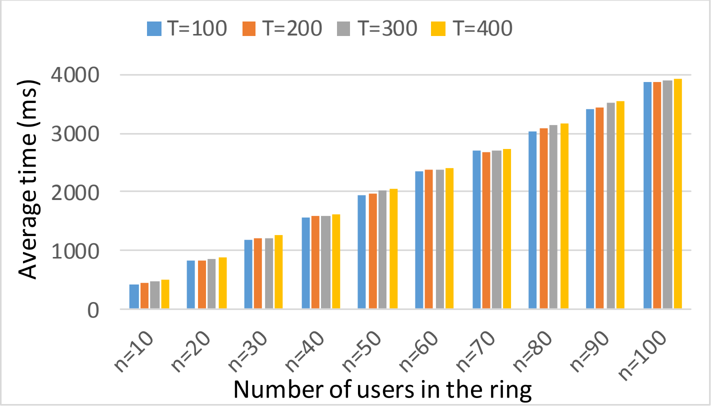

Chart -1: Time for Service provider to verify ring signature |N|=1024

A comparison of number of granted keys between three methods is shown in chart 2. If we grant the key one by one, the number of granted keys would be equal to the number of delegated cipher text classes. With tree based structure, we can save a number of granted keys according to the delegation ratio. In our proposed approach the delegation of decryption can be efficiently implemented with the aggregate keys which is only fixed size. In our system delegation is randomly choose. It models the situation that needs for delegation to different users may not be predictable as time goes by even after a careful initial planning.

The test machine is a laptop personal computer equipped with 2.50 GHz Intel CPU with 4 GB RAM and running windows 7 operating system. The timing reported below are averaged over 100 randomized runs. As shown in Table 5 the execution time of setup, key generation, and encrypt are independent of the delegation ratio r. in our system key generation takes 3.3 milliseconds and encrypt takes 6.8 milliseconds. The running time complexity of encrypt and decrypt increase linearly with delegation ratio r.

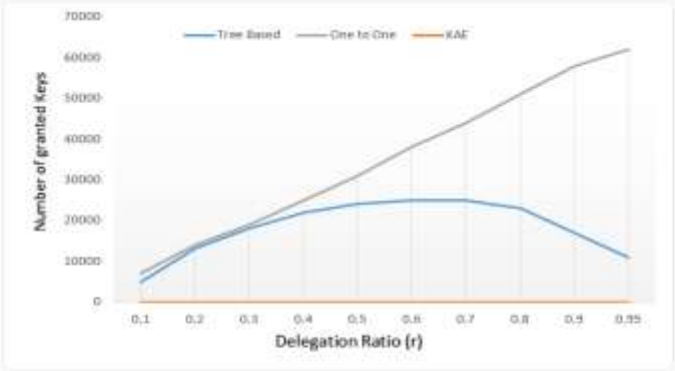

Chart -2: Number of granted keys

3. Mathematical Model

Input:

Let S is the Whole System Consist of S={Us, DO, F, TPA, CS}, Where F is Collection of documents which created by owner F= {f1, f2, ….. , fn}, f1, f2 = no of files, Us= no of Users, Us={u1,u2,….. un}, DO= data owner, Do={PID,SR,RS,E,U}, PID= public id of users, SR=setup ring, RS=ring signature, E-Extract, U- Update, TPA={C, V, P}, C=challenge, V= verify, P= proof by server, CS= cloud server

Procedure:

The proposed system mainly consists of the following five stages:

- Stage 1: Setup (S) - On input a unary string 1L, where L is a security parameter, the algorithm outputs a master secret key msk for the third party PKG (Private Key Generator). A list of system parameters param that includes L and the descriptions of a user secret key space D, a message space M as well as a signature space.
- Stage 2: Extract (E) – On input a list param of system parameters, an identity IDi € (0, 1)* for a user the master secret key msk, the algorithm outputs the user's secret key $sk_{i,0}$ € D such that the secret key is valid for time t=0. We denote time as non-negative integers. When we say identity Idi corresponds to user secret key $sk_{i,0}$ or vice versa, we mean the pair (Idi, $sk_{i,0}$) is an input-output pair of Extract with respect to param and msk.
- Stage 3: Update (U) - On input a user secret key $sk_{i,t}$ for a time period t. The algorithm outputs a new user secret key $sk_{i,t+1}$ for the time period t + 1.
- Stage 4: Sign (S1)- On input a list param of system parameters, a time period t, a group size n of length polynomial in ƛ, a set L = {ID$_i$ €(0,1)* | i € [1, n] } of n user identities, a message m € M, and a secret key $sk_{\prod+1}$€ D , π €[1,n] for time period t, the algorithm output a signature σ € Ψ .
- Stage 5: Verify (V) - On input a list param of system parameters, a time period t, a group size n of length polynomial in ƛ, a set L = {ID$_i$€ (0, 1)* | i € [1, n]} of n user identities, a message m € M, a signature σ € Ψ. it outputs either valid or invalid.
- Stage 6: Public Audit:
  The cloud servers and TPA interact with one another to take a random sample on the blocks and check the data intactness in this procedure.
  Challenge (F info) → (C): This algorithm is performed by the TPA with the information of the file F info as input and a challenge C as output.
  Proof Gen(C, _) → (P): This algorithm is run by each cloud server with input challenge C, coded block set and authenticator set then it outputs a proof P.
  Verify (P, pk, C) → (0, 1): This algorithm is run by TPA immediately after a proof is received. Taking the proof P, public parameter pk and the corresponding challenge C as input, it outputs 1 if the verification passed and 0 otherwise.
- Output (O) A (1, n) should satisfy the verification correctness signatures signed by honest signer are verified to be invalid with negligible probability

4. CONCLUSIONS

Propelled by the down to earth needs in data sharing, we proposed another idea called Authentic and Anonymous Data Sharing with Enhanced Security. It permits an ID-based ring signature plan to have enhanced secure key. It is the first in the writing to have this element for ring signature in ID-based setting where multiple rings are generated to share the data and every ring have multiple users of group. Our plan gives unqualified obscurity also, can be demonstrated forward-secure unforgettable in the arbitrary prophet model, accepting RSA issue is hard. Our plan is exceptionally effective and does not require any pairing operations. The extent of client mystery key is just one whole number, while the key overhaul prepare just requires an exponentiation. We trust our plan valuable in numerous other useful applications, particularly to those require client protection and validation, for example, impromptu system, e-business exercises and keen network.

Access control is very important scope and in our system only eligible users can have the access to the data so the main future focus is on every user can have access of data and also our present plan depends on the arbitrary prophet suspicion to demonstrate its security. We consider a provably secure plan with the same elements in the standard model as an open issue and our future examination work.

REFERENCES

[1] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multicloud architectures," IEEE Trans. Dependable Sec. Comput., vol. 10, no. 4, pp. 212–224, Jul.\Aug. 2013.

[2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute- based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[3] S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui, "Efficient identity based ring signature," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Security, 2005.

[4] 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.

[5] 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.

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

[8] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multicloud architectures," IEEE Trans. Dependable Sec. Comput., vol. 10, no. 4, pp. 212–224, Jul.\Aug. 2013.

[9] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute- based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[10] 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.

[11] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring distributed accountability for data sharing in the cloud," IEEE Trans. Dependable Secure Comput., vol. 9, no. 4, pp. 556–568, Jul./Aug. 2012.

[12] Y. Wu, Z.Wei, and R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," IEEE Trans. Multimedia, vol. 15, no. 4, pp. 778–788, Jun. 2013.

[13] S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui, "Efficient identity based ring signature," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Security, 2005.

[14] J. Camenisch. Efficient and generalized group signatures. In EUROCRYPT 97, volume 1233 of Lecture Notes in Computer Science,pages 465–479. Springer, 1997.

[15] N. Chandran, J. Groth, and A. Sahai. Ring signatures of sublinearsize without random oracles. In ICALP 2007, volume 4596of Lecture Notes in Computer Science, pages 423–434. Springer, 2007.

[16] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana. Social cloud computing: A vision for socially motivated resource sharing. IEEET. Services Computing, 5(4):551–563, 2012.