An Efficient Technique for Authentic and Anonymous Data Sharing with Forward Security

Sakeena P T[1], Bini K B[2], Girish R[3]

[1]M. Tech, [2,3]Assistant Professor

Computer Science and Engineering, Nehru College of Engineering and Research Centre, Trissur, Kerala, India

Abstract*— Data sharing is not an easier job with the advancement of internet-based applications and cloud computing. Data sharing provides a number of benefits to people and society. In a data sharing system with a group of users, the data owner has led to several kinds of security related issues such as efficiency, data integrity and privacy of the data owner. An authentic and anonymous data sharing system is required to protect the privacy of the data owner. Ring signature is a cryptographic technique which ensures authenticity and integrity of the digital data. It can be defined as a type of digital signature which helps the data owner to construct a secure and anonymous data sharing system. A data owner can send his data on the behalf of a group. The traditional public key infrastructure (PKI) includes the verification of certificates which is both cost and time consuming process. Identity-based (ID-based) ring signature makes the process of verification more efficient and it does not require any validation of digital certificates. Introduction of forward security along with the ring signature also enhances the security of the system. It also uses an efficient secure hash algorithm with RSA which provides better execution time and less system overhead as compared with the existing ring signature schemes.

Keywords: Data Sharing, Authentication, Anonymity, Ring signature, Forward Security.

I. INTRODUCTION

In Cryptography, ring signature is defined as a type of digital signature which provides signer's anonymity. It can be performed by any member of a group of users that each group member have keys. Ring signature is a ring- like structure and it is similar to a group signature but it differs in two ways: First, there is no way to revoke the anonymity of the signer of the message and second, any group can be used as a group without additional set up. Unlike group signatures, the ring signature requires no group manager, no member revocation and it is spontaneous. Anonymity is one important form of privacy protection. This technique can maintain the anonymity of real signer. No one can reveal real signer's anonymity.

This system combined the advantages of two techniques i.e. ID-based cryptosystem and the ring signature [7]. In traditional public key based ring signature verifier first validate the certificates of every user, then only he can verifies the message and signature pair. But in ID-based ring signature only the identities of ring members together with message and signature are needed for verification. ID-based cryptosystem eliminate the need for verifying certificates of each member of a ring which is both cost and time consuming process. The public key of each user is computable from user's publicly known identity such as email address, residential address etc. A Private Key Generator (PKG) is a master entity in an organization who computes private keys from its master secret for every users. Private Key Generator uses some secret information to compute the secret keys related to the identity of the user. This secret key sent to the user throughout a secure channel.

Every digital signature schemes have a problem of key exposure. If the private key of any user is leaked, all the signatures created by it become worthless. Validation of future signatures will be failed. Somebody can steal your secret key when your computer is infected with Trojans, or when you use the same secret key in a publishing website. Introduction of forward security to the ring signature effectively enhances its security feature. A forward secure signature in the past time slot remains secure even if the current secret key is lost. Dividing the lifetime of a public key into 'T' time intervals and in each time interval the same public key corresponds to a different secret key. When a secret key is leaked, all the previously generated signatures remain valid and not need to be regenerated.In recent years, several kind of ID-based ring signature schemes have been proposed and they are based on bilinear pairing algorithm. But this system is an ID-based signature scheme whose security relies on Rivest, Shamir and Adelman (RSA) problem which is an asymmetric cryptographic technique used to produce primitive digital signatures. The basic RSA scheme is not very secure. So a Random Oracle Model (ROM) is applied to this system. In order to prevent the attacks, first apply the cryptographic hash function to the message m to form a message digest, then apply the RSA algorithm to produce the signature. It increases the efficiency, compatibility and integrity. By verifying the signature one can be assured that the message is given by a valid user while cannot identify who is the actual signer of the message. Hence the anonymity of the data owner is ensured together with data authenticity and data integrity. Hence verification is very efficient, it does not involve any certificate verifications. Ring signature provides signer's anonymity and also ensure the authenticity and integrity of the message shared among the users.

II. SYSTEM MODEL

An authentic and anonymous data sharing system ensures the privacy of the data owner and provides signer's anonymity. A data owner first set up a ring by choosing number of persons to his group, it need only the public identity information of the ring members. Owner can upload his personal data to the data center along with the ring signature. By verifying the signature one can identify that the message is given out by a group member, but cannot find that who the actual signer of the message. In this way the system ensures the authenticity and anonymity. This system also supports the forward security feature which enhances the security of the system. In [5] the following figure Fig.2.1 shows an ID-based ring signature scheme in which the Bob is the data owner. Bob can upload his personal data together with ring signature on behalf of a group. By verifying the signature one can find that the message is send by a ring member, cannot identify the Bob's identity. In this way the system assures the signer's anonymity.

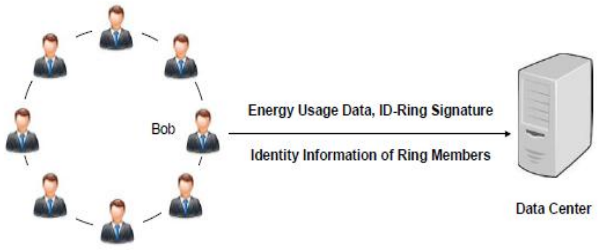

Bob
Energy Usage Data, ID-Ring Signature
Identity Information of Ring Members
Data Center

Fig. 2.1 ID- based Ring Signature

III. PREVIOUS WORK

A. *ID-based Blind Signature and Ring Signature using Bilinear Pairings.*

F. Zhang and K. Kim introduced an ID-based Blind signature and Ring signature from bilinear pairings [1]. Bilinear pairing is defined as a kind of maps that can be constructed on some elliptic curves. This method is secure in random oracle model. Blind signatures and Ring signatures are very useful to provide user's anonymity and privacy. The security of an ID-based blind signature scheme consists of two requirements. They are the blindness property and the non-forge ability of additional signatures. It is playing an important role in building e-commerce. User's anonymity is protected by means of blind signature and signer's anonymity is protected by group or ring signature.

Bilinear Pairing Algorithm:

Let G be a cyclic group whose order is q. V be a cyclic multiplicative group of same order q. Then e: G×G→V. It is called bilinear pairing which satisfies the following condition.

Bilinear: e (P_1+P_2Q)=e (P_1Q) e (P_2Q) where `e` is a bilinear map.This scheme can be performed with super singular elliptic curves or hyper elliptic curves. The essential operation in this technique is only the computation of bilinear pairings. It also uses compression techniques to reduce length of the signature. But this scheme is based on identity rather than the arbitrary number, a public key consists of some aspects of user's information which may uniquely identify himself. It is not that much efficient against generic parallel attacks.

B. *Forward Secure Ring Signature and Key Insulated Ring Signature Schemes.*

J. K. Liu and D. S. Wong introduced Solutions to key exposure problem in ring signature [2].This system suggests a solution to the key exposure problem. It proposed a first forward secure ring signature scheme and a key insulated ring signature scheme. It allows a (t, n) threshold settings. Even if 't' secret keys are compromised, the validity of all the forward secure ring signatures generated in the past still preserved. The key insulated concept is almost similar to forward security. In this scheme the life time of a secret key is divided into discrete time periods and even a secret key is compromised, the attacker cannot generate valid signatures in future time periods using the compromised secret key. It reduces the risk of key exposure. Both schemes are secure in random oracle model. But in this scheme the size of signature grows linearly with the number of users. So need to make a constant size.

C. *ID-based Threshold Linkable Ring Signature Scheme.*

P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong introduced A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity[3]. This is the first ID-based threshold linkable ring signature scheme and it allows anyone to tell whether the two signatures are produced by the same signer by using the same private key. But in this scheme identity is not preserved. It supports t-out-of-n threshold settings. Threshold ring signatures proposed that t parties can compute a (t, n) ring signature σ on a message m (m, Si1, Si2, Si3 $_{\ldots}S_{it,}$ $P_{1,}$ $P_{2\ldots.}$ $P_{n.}$). This scheme does not support any forward secure mechanism. If the private key of a signer is compromised, all the signatures become worthless.

D. *Forward Secure Ring Signature without Random Oracles.*

J. K. Liu, T. H. Yuen, and J. Zhou introducedforward secure ring signature without random oracles [4]. This system tells that the signature in the past time slot remains secure even if the current secret key is lost. Main idea is that dividing the lifetime of the public key into 'T' time periods and in each time period the same public key corresponds to different secret keys. This scheme uses the assumptions of Computational –Diffie Hellman (CDH) and subgroup decision. Without random oracle signature size is hugeand it also based on a traditional public key settings therefore it involves expensive certificate check [6]. In a forward secure signature scheme, if the knowledge of the secret key at a particular point in time does not help to forge signatures relative to the previous time periods. In addition, the size of the secret key , the public key and the signature should not be depend on the number of time period during the lifetime of the public key. A forward secure ring signature scheme has a number of applications in wireless sensor networks and smart grid systems.

E. Cost Effective Authentic and Anonymous Data Sharing with Forward Security.

Xinyi Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang introduced cost effective authentic and anonymous data sharing with forward security[5]. It proposed a forward secure ring signature scheme whose security relies on RSA problem. This scheme eliminates the process of certificate verification and also enhances the security of ID-based ring signature by providing forward security.It is an ID-based setting with size of secret key is only one integer. This scheme uses a 1024 RSA bit key level and the secret key is also 1024 bits. Every key updating requires just an exponentiation and the signing and verification process do not require any pairing in any stage.

IV. PROPOSED METHODOLOGY

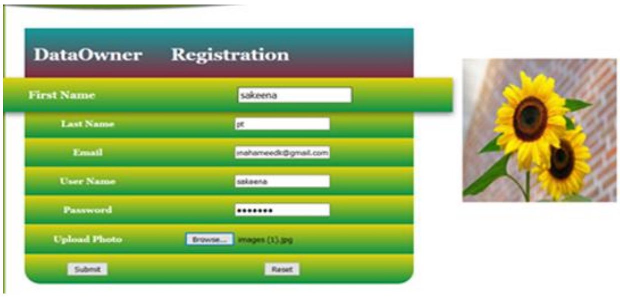
The proposed work combined the advantages of two techniques: ID based cryptosystem and the ring signature. The basic process will be: Users registered and authenticated into the system. Data Owner creates a group and he add some members to his group. Once it is done the system will generate a secret key for every user. Owner who wants to share the data has to sign it by using an ID-based signature. Based on the user information and the document information, the signature will be calculated. To access a particular data by some user, verify the signature of the document by using the public key. Signature of the document and the generated signature will be checked. If it is same, then the document is accessible to user.

Data ownerfirst sets up a group or ring by choosing a group of users. For this owner does not need any collaboration from any ring members and only needs the user's public identity information. User contacts a private key generator (PKG), a master entity who computes secret key for every users and this key throughout a secure channel. This secret key is valid for a particular time period after that the key will be expired which ensures forward security.

Proposed System Modules:

A. User Registration and Authentication:

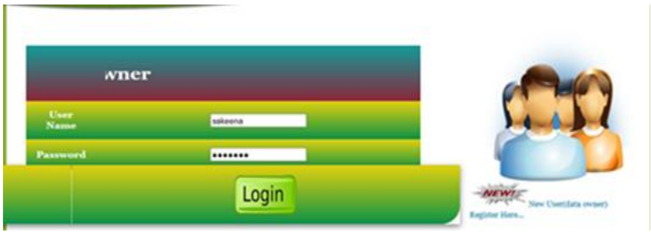
In this module user has to register into the system. To register user has to fill all the registration details that is first name, last name, username, password, email id etc. as shown in Fig.4.1. User need to enter all the valid information, after that he can login to the system by using his own username and password.



DataOwner Registration

First Name: sakeena
Last Name: pt
Email: inahameedk@gmail.com
User Name: sakeena
Password: •••••••
Upload Photo: images (1).jpg

Fig.4.1 User Registration



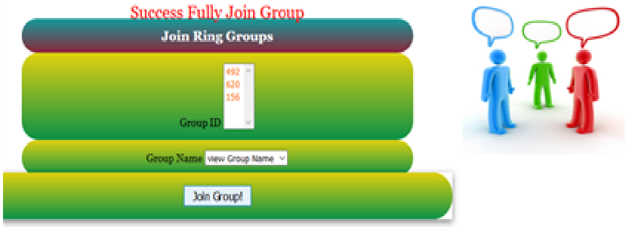
wner

User Name: sakeena
Password: •••••••

Fig.4.2 Authentication

B. Group Creation:

Data owner first sets up a group or ring by choosing a group of users. For this owner does not need any collaboration from any ring members and only needs the user's public identity information. Owner select a group id and a group name and successfully join to a group as shown in Fig.4.3



Success Fully Join Group

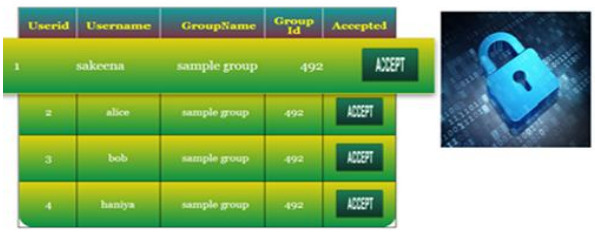
Join Ring Groups

Group ID: 492
620
156
Group Name: view Group Name

Fig. 4.3Group Creation

C. Private Key Generator:

User contacts a private key generator (PKG), a master entity who computes secret key for every users and this key throughout a secure channel to the corresponding email id of the user which is used to upload the file. This secret key is valid for a particular time period after that the key will be expired which ensures forward security.



Userid	Username	GroupName	Group Id	Accepted
1	sakeena	sample group	492	ACCEPT
2	alice	sample group	492	ACCEPT
3	bob	sample group	492	ACCEPT
4	haniya	sample group	492	ACCEPT

Fig.4.4 Private Key Generation

D. Ring Signature:

Suppose a group of entities, each member have a public/private key pairs, (P1, S1), (P2, S2) ... (Pn, Sn). Member i can compute the ring signature σ on a message m with input (m, Si, P1, P2… Pn). Anyone can verify the validity of the ring signature σ, m and the public keys P1, P2… Pn. It is hard to create a valid ring signature on a message m without knowing any of the secret key.Data Owner can upload his personal data along with the ring signature and the generated public key. This scheme using a RSA key pair generator which produces a public key and a private key. Private Key is used to produce the signature and the generated public key is used to verify the signature. Public key is generated from the public identity information of the ring members. So the verifier can be assured that the message is given by a group member but he cannot identify who the actual owner of the message. In this work SHA1withRSA algorithm is used to produce the signature and the public key. Both are in cipher text form. It also uses a secure random method to produce a message digest. Signature is applied to the digest form of the message and share the data with others. The following algorithms are used to produce the signature.

RSA Algorithm:

Generate a RSA key pair contains a modulus N, i.e. the product of two large primes. Consider two integers e and d where ed=1(modϕ(N). Signer's public key contains N and e and the signer's secret key contains d. To sign a message m, signer computes the following equation:

$$\sigma = m^{d}\,(\text{mod } N) \tag{1}$$

To verify a message, the receiver has to check the following equation:

$$\sigma^{e} = m\,(\text{mod } N) \tag{2}$$

The basic RSA scheme is not very secure. RSA operation cannot handle messages longer than the modulus size. If a 2048bit RSA key, it cannot able to directly sign any messages longer than 256 bytes long. So a cryptographic hash function can take an arbitrary long message and then compress it into a short string. So signing a hash is as good as signing the original message.

SHA1RSA Algorithm:

SHA1RSA is a message digest algorithm which using hash functions to hash the package with SHA (Secure Hash Algorithm). Then it yields a small 20 byte hash string known as message digest and it can computed very fast. Sign the hash string with the private key to prove that the message is come from the owner. An SHA1RSA scheme is very secure because an attacker required 2^{160} operations to leak the original message. So it is very fast and secure than MD5 which is also a message digest algorithm that produces 128 bit output. In this algorithm, a signature object can be used to generate and verify digital signatures. There are mainly 3 phases to use a signature object for signing and verifying a signature.

Initialization:

A public key will be initializes the signature for verification and a private key generated by a secure random number generator will be used to initialize a signature for signing.

Updating:

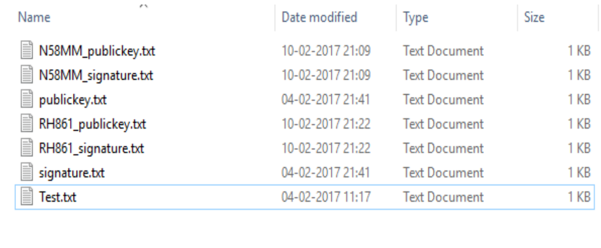
In this phase, updating the bytes to be signed or verified by using update method.

Signing or verifying:

In this phase, signing or verifying the signature on all the updated bytes by using corresponding sign and verify methods. RSA signature size is depends on the key length which is the length of the modulus 'N' in bytes. This means 'n' bit key the resulting signature also will be 'n' bits long or exactly 'n' bits. RSA key length ranges from 1024 bits and more.

E. Upload Data:

When uploading a file a public key and a signature is produced and writes it into two files as shown in Fig.4.5. Share the file along with the signature.Signature is often produced as a Hexadecimal number but it can be written in Base 64 to ASCII encoding.

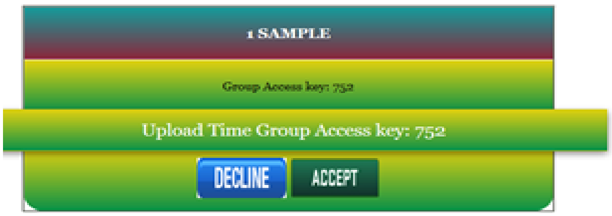


Name	Date modified	Type	Size
N58MM_publickey.txt	10-02-2017 21:09	Text Document	1 KB
N58MM_signature.txt	10-02-2017 21:09	Text Document	1 KB
publickey.txt	04-02-2017 21:41	Text Document	1 KB
RH861_publickey.txt	10-02-2017 21:22	Text Document	1 KB
RH861_signature.txt	10-02-2017 21:22	Text Document	1 KB
signature.txt	04-02-2017 21:41	Text Document	1 KB
Test.txt	04-02-2017 11:17	Text Document	1 KB

Fig. 4.5GeneratePublic key and the Signature writes into two Files.

F. Verifying Phase:

Message is uploaded along with the ring signature and the public identity information of the user.Every uploaded data has to be verified before sharing to other users. So Verifier checks that the message is given by a valid user. For this, system verifies the Group access key and key in the upload time is same or not. Moreover it verifies the signature produced and the signature of the document. If all the equalities hold, the system will accept the file otherwise decline.



1 SAMPLE

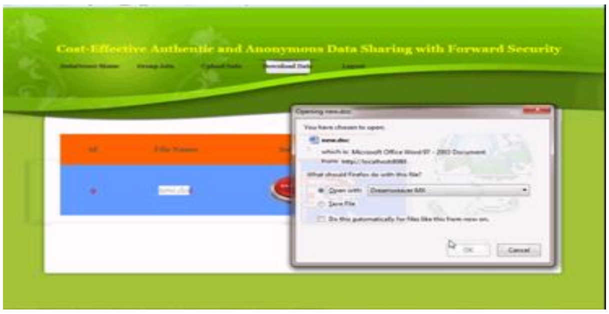
Group Access key: 752

Upload Time Group Access key: 752

Fig.4.6 Verifying Data

G. *Data Retrieval:*

The system will calculate the signature of the document and check the signature of the document and the generated signature is same. If it is the message is accessible to user. Once the signature is verified by the system, the document is accessible to the user and it is available for download.



Cost-Effective Authentic and Anonymous Data Sharing with Forward Security

You have chosen to open:

which is: Microsoft Office Word 97 - 2003 Document

What should Firefox do with this file?

○ Open with

○ Save File

□ Do this automatically for files like this from now on.

Fig.4.7Data Retrieval

The following table shows the comparison of existing ID-based signature schemes and the proposed method.

TABLE I. COMPARISON WITH OTHER ID-BASED RING SIGNATURE SCHEMES.

Reference paper	**Techniques Used**	**Pros**	**Cons**
[1]	ID-based blind signature and ring signature using bilinear pairing algorithm.	Efficient key management, Moderate security, Length of the signature can be reduced.	Based on identity rather than an arbitrary number, No efficient against generic parallel attacks.
[2]	Forward secure ring signature and key insulated ring signature schemes.	Forward security, Minimize the damage of key exposure.	Size of signature grows linearly along with the number of users.
[3]	A non-pairing ID-based threshold ring signature scheme.	Elimination of certificate verification saves the computation and communication cost.	Key exposure, No forward mechanism. If the private key is compromised all the keys remain worthless.
[4]	Forward secure ring signature without random oracles.	Forward security.	Signature size is huge.
Proposed scheme	A ring signature scheme which allows user to sign anonymously on behalf of a group.	Scheme is proven secure in RSA and random oracle model. Forward security.	SHA1RSA is secure but it is more complex.

V. EXPERIMENTAL RESULTS

The following experiment analyses the performance of the system. SHA1RSA Authenticates faster and it takes 500ms for verification. Here the following graphs shows the performance of the system as a result of the experiments conducted to the system.

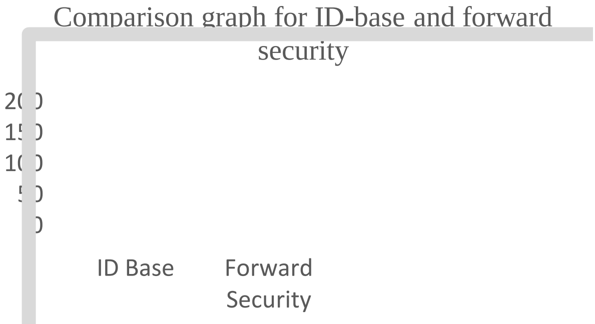


Fig.5.1 Comparison graph for Id-based and id-based with forward security.

The below graph Fig. 5.1 shows the comparison between id-based ring signature and the id-based ring signature with the forward security. When a user compromise the secret key at a particular time slot, in case of an id-based scheme without forward security all the signatures produced by using this secret key become invalid and future signatures cannot be generated. Due to this access to the previously uploaded files will be restricted. But, in case of forward security even if a key is compromised, all the files signed by using this key is remain valid and it will not affect the system. User only restrict the access to the file which has been uploaded at the current time slot.

Second graph Fig. 5.2 shown below is for the file uploading time i.e. the time required to sign a file by a user and the secret key generation for user. Here considering the last 5 files and its uploading time in milliseconds.

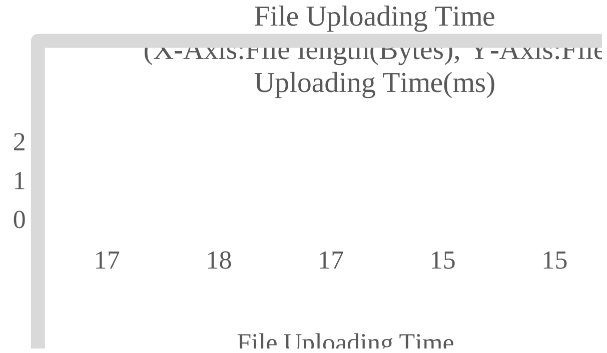


Fig. 5.2 File Uploading Time

Next graph Fig. 5. 3 shown below is for file downloading time i.e. the time required for verification and downloading of files. Here also consider the last 5 files and the download time for the corresponding files.

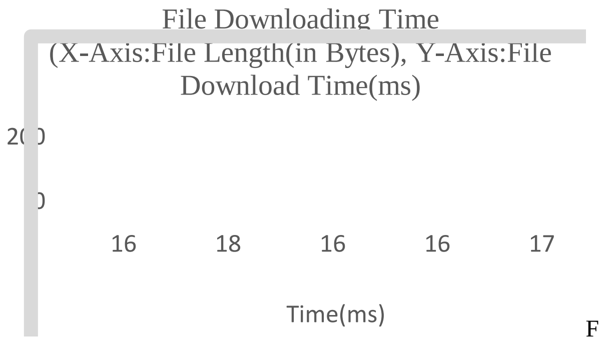


Fig.5.3. File Downloading Time

VI. CONCLUSION

This paper reviews various existing ring signature schemes and introduced a forward secure ID-based ring signature scheme which combines both ID based cryptosystem and the ring signature techniques. It provides a good solution for the key exposure problems. The forward secure signature was proposed for preserving the trustworthiness of past signatures even if the current secret key is compromised. In this scheme, the size of the secret key is just one integer and it does not require any complex pairing operations. This scheme will be very useful in many other practical applications including ad-hoc network, e-commerce websites and smart grid systems. User privacy and authentication must be required in these systems. This scheme provides unconditional anonymity and proven secure in the random oracle model under the standard RSA assumption. This scheme using a secure hash algorithm with RSA (SHA1RSA) has improvement inexecution time as compared to the existing techniques.

VII. FUTURE SCOPES

We will consider with this secure hash scheme with the same features in a standard model as an open problem and our future work.

REFERENCES

[1] F. Zhang and K. Kim., "ID-Based blind signature and ring signature from Pairings", In ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 533–547. Springer, 2002.

[2] J. K. Liu and D. S. Wong, "Solutions to key exposure problem in ring signature", I. J. Network Security 6(2):170–180, 2008.

[3] P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong, "A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity (extended abstract)", In Prov Sec, volume 6402 of Lecture Notes in Computer Science, pages 166–183. Springer, 2010.

[4] J. K. Liu, T. H. Yuen, and J. Zhou, "Forward secure ring signature without random oracles", In ICICS, volume 7043 of Lecture Notes in Computer Science, pages 1–14. Springer, 2011.

[5] Xinyi Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, "Cost effective authentic and anonymous data sharing with forward security", IEEE Transactions on computers vol:64 no: 6, 2015.

[6] Shacham and B. Waters, "Efficient ring signatures without random oracles", In Public Key Cryptography, volume 4450 of Lecture Notes in Computer Science, pages 166–180. Springer, 2007.

[7] A. Shamir,"Identity-Based Cryptosystems and Signature Schemes",In CRYPTO 1984, volume 196 of Lecture Notes in Computer Science,pages 47–53. Springer, 1984.

[8] National Institute of Standards and Technology. NIST IR 7628: "Guidelines for Smart Grid Cyber Security", August 2010.

[9] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage", IEEE Trans. Computers, 62(2):362–375, 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., 24(6):1182–1191, 2013.