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. 4, Issue 6, June 2016

A Well Secure and Cost Efficient Mechanism for Sharing Data using Forward and Backward Security

Pritee Raut[1], S.B.Natikar [2]

P.G. Student, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, India[1]

Assistant Professor, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, India[2]

ABSTRACT: In Cloud Computing Sharing of data is troublesome when various clients share an information on cloud. Ring Signature is valuable to make secure data sharing on cloud .In Ring Signature clients confirm their information which is put away on cloud, but Certificate Verification in Ring Signature is Costly. So this User Identity Based Ring Signature is utilized to maintain a strategic distance from the Process of Certificate Verification. Security level of User identity based Ring Signature is enhances by giving Forward Security. Due to the Forward Security if a Secret key of any user is disclosed by attacker then all Previous Signatures of that signer remain Secure. In Our System, We further increases Security of Forward Secure Identity based Ring Signature by providing Backward Security: Even if we revoke any person, they are able to access the existing files so that to defeat this issues our Proposed framework Provide confinements on client which we deny to get the current records.

KEYWORDS**:** Authentication, Data Sharing, Cloud Computing, Forward Security, Backward Security

I. INTRODUCTION

A Well Secure and Cost Efficient authentic mechanism provide forward as well as backward security to sharing of data on cloud.Ring Signature: In a Ring Signature scheme[2] the one participant of ring signs a document and send that document to all participants of ring.The participants of ring who accept the document does not know who is the real signer in ring.There is no need of communication between participants of ring.but there is problem of key leakage in ring signature[1]. Attacker may steal the secret key if computer is infected with Trojans.

Forward Secure Ring Signature:

For key leakage problem in ring signature Forward Security was designed for ring signature[3].Forward secure ring signatures of signer in past remains valid even if current secret key is lost. Forward Secure Ring Signatures were proposed by Liu and Wong in 2008[4] to resolve the problem of key leakage in ring signatures.The motivation of this technique is to reduce the damage caused by leakage of any secret key of users in ring signature.

Proposed System Provide backward security to data sharing on cloud. Backward security restrict the system if we revoke any user from accessing the files. With this, we accomplish forward as well as backward security. We utilize the idea of hash chain in the computerized signature.This guarantees the strong security of the mark, furthermore guarantees that future marks are not compromised during lekage of secret key.

ID-based ring mark is by all accounts an ideal tradeoff among proficiency, information credibility and namelessness, furthermore, gives a sound arrangement on information imparting to a expansive number of members. To acquire a greater aggregate confirmation,one can incorporate more customers in the ring.In any case, doing this builds the possibility of key introduction too.Key presentation is the significant obstruction of standard propelled marks.On the off chance that the private key of an underwriter is traded off, all marks of that endorser get to be useless: future marks are discredited and no beforehand issued marks can be trusted. When a key spillage is recognized,key repudiation instruments must be conjured quickly keeping in mind the end goal to keep the era of any mark utilizing the traded off mystery key.Not with standing, this does not take care of the issue of forgeability for past marks.The thought of forward secure mark was proposed to protect the legitimacy of past marks regardless of the fact that the current mystery key is bargained. The idea was initially proposed by Anderson[12], and the arrangements were composed by

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. 4, Issue 6, June 2016

Bellare and Miner [13].Proposed System is inspired by the Security of future secret keys.In existing system once the secret is uncovered, the security of the past mystery keys can be ensured, but that of the future secret keys is compromised. In other words, the future secret keys can be copied fraudulently and if the original signer cannot detect that duplicate future secret keys, it is consider as a total breakdown of the system. Therefore, the perfect solution would be distinguish such an interruption and after that change the keys.

II. RELATED WORK

R.Gupta and Tanisha [5] contributed the concept of file security model which uses the concept of hybrid encryption scheme to meet security needs. In this model, encryption and decryption of files at cloud server is done using blowfish and modified version of RSA.

E. Abd, Al Latif ,Al Badawi and A. Kayed [6] provides the achievable security merits by making use of multiple distinct clouds simultaneously.Different distinctive models are acquainted and talked about concurring with their security and protection abilities and desires.

S.Subbiah,S.Selva and T. Ramkumar [7] spoke to a methodology for Enhancing Secure Cloud Storage Using Vertical Partitioning Algorithm.The vertical dividing calculation is utilized to ensure the information in a productive way. The calculation has been executed in a java stage and results are contrasted and alternate calculations.

P.Raut,V.Baporikar [8] intends to outline and Implementation of Enhanced Security in Multicloud Storage System Using Distributed File System.In this framework, they are executing the thoughts of different distributed storage adjacent to with improved security utilizing encryption techniques generally putting away finish record on single cloud framework.

J.K.Liu, T. H.Yuen, and J. Zhou[10], propose a forward secure ring mark plan without arbitrary oracles.With forward security, if a mystery key of a relating ring part is uncovered, all beforehand marked marks containing this part remain valid.This is particularly helpful on account of ring mark, as the presentation of a solitary mystery key might bring about the invalidity of thousands or even millions ring marks which contain that specific client.

Ai fen Sui, Sherman S.M. Chow[12] proposed, a detachable and unknown ID-based key issuing protocol.If the convention unveil the data about who has asked for his/her mystery key and who has not, the genuine quality will be influenced.

Man ho Au,Joseph K .Liu [13] develop ID based Ring mark plan in standard model.They use Diffie Hellman suspicion. This plan shuts the open issue of outlining an ID-based ring mark utilizing uncomparable quantities of matching calculation to expand the proficiency of information sharing.but this plan does not give in reverse security to information in distributed computing.

III. BACKWARD SECURITY

In existing System they focus on forward security but they are unable to provide backward security.Due to this Problem Backward Security is Provided.In existing system even if we revoke any person in ring, they are able to access the existing files. So that to overcome this our new system will provide restrictions on users which we revoke to access the existing files. Ex.If there are ten users in ring and we provide forward security to all the members of ring.After that we decide to revoke two users of ring. For that we have to remove forward security constraints of these two users and provide restrictions on these two users for accessing existing files.For implementing this our proposed system will uses backward security.Quality of Security in our system is enhances while sharing of data on cloud.

This mechanism uses Elliptical curve Cryptography Algorithm for key generation ,encryption and decryption process. Key generation is an important part where both public key and private key will be generated. The primary benefit promised by Elliptical curve Cryptography is a smaller key size, reducing storage and transmission requirements.

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. 4, Issue 6, June 2016

IV. EXPERIMENTAL RESULTS

The computation complexity of algorithms of our scheme are shown in Table 1.

TABLE 1
Computation complexity of algorithms

	Exponentiation	Multiplicative inverse	Multiplication	Hash
Setup	-	-	1	-
Extract (for 1 user)	2	1	1	1
Update	1	-	-	-
Sign	$3 \times n \times \ell/\ell'$	-	$(2 \times n - 1) \times \ell/\ell'$	$n \times \ell/\ell'$
Verify	$(n+2) \times \ell/\ell'$	-	$(2 \times n - 1) \times \ell/\ell'$	$n \times \ell/\ell'$
Revoke	O(n)	O(n)	O(n)	O(n)

Notation:

n: number of users in the ring;
ℓ': length of the output of hash function in the scheme;
ℓ: length of the output of a secure hash function (usually it is 160);
O(n) : Time required to revoke n user

The space requirement of our scheme is shown in Table 2.

TABLE 2
Space requirement

	Space required
Public parameters	$\mathcal{O}(1)$ (4 integers + descriptions of 2 hash functions)
Secret key	$\|N\|$ bits
Signature	$(n \times (\|N\| + \ell') + \|N\|) \times \ell/\ell'$ bits

Notation:
N: RSA modulus;
$|N|$: the length of N in binary bits;
n: number of users in the ring;

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

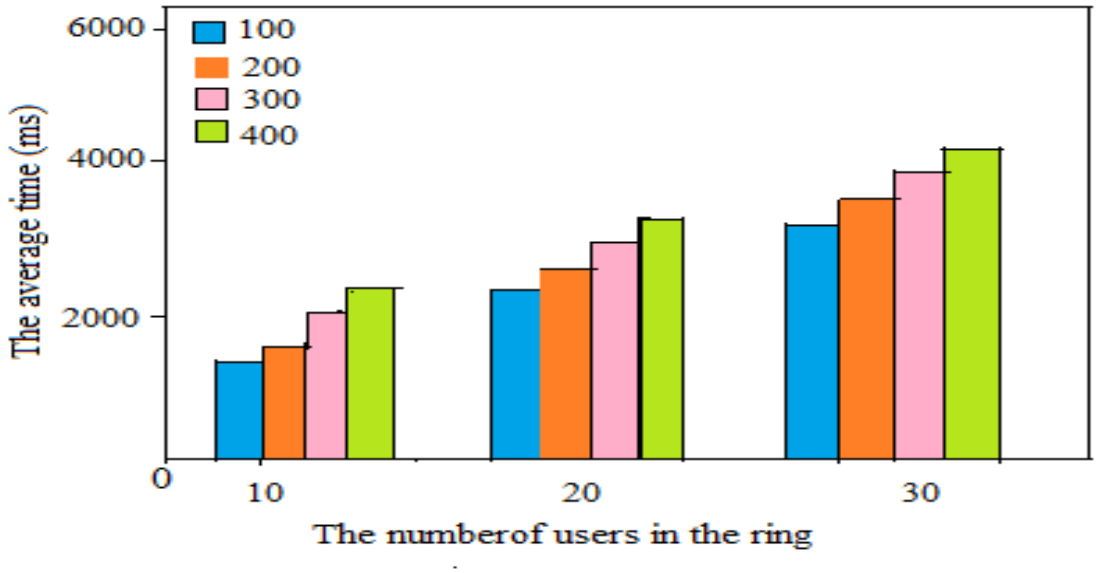
Vol. 4, Issue 6, June 2016

Following Fig.1 shows no.of users in ring and average time for data owner to sign energy data usage data, We calculate this average time for data owner to sign energy usage data by using the formula, Sign=3 * n * l/l' Where,n=Number of users in ring,l =Length of secure function(usually it is 160) and l'= Length of hash function in our scheme.i.e 16

Unit : ms

	T=100	T=200	T=300	T=400
n=10	300	603	810	1006
n=20	600	1150	1585	2050
n=30	900	1780	2415	3102
n=40	1200	2280	3040	3980

a)



(b)

Fig.1 The average time for the data owner to sign energy usage data, |N| = 352 bit

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

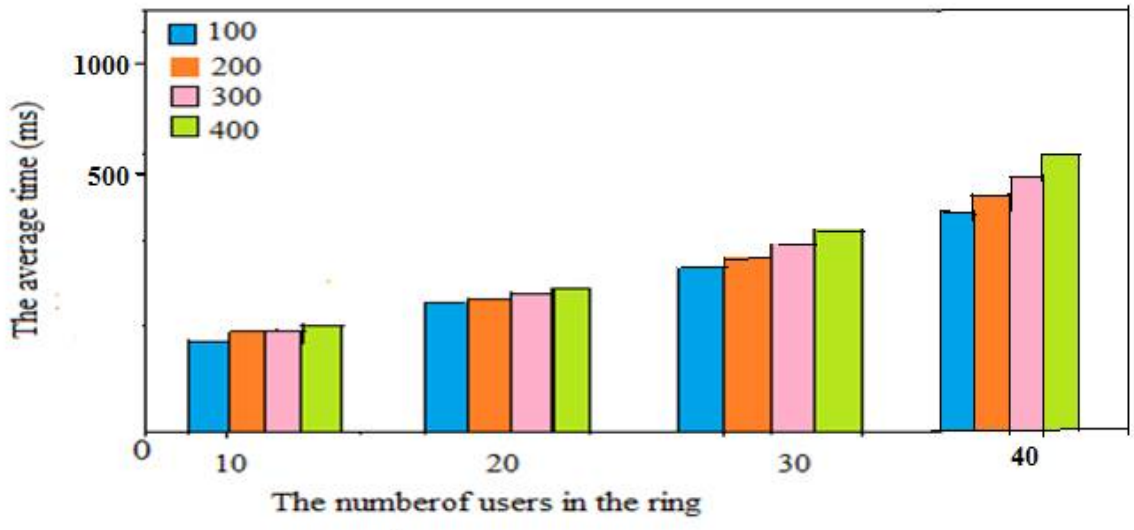
Vol. 4, Issue 6, June 2016

Following Fig. 2 shows the no of users in ring and the average time for the service provider to verify the ring signature, We calculate this average time for service provider to verify the ring signature by using the formula,
Verify=(n+2) * l/l'
Where,n= Number of users in ring,l=Length of secure function,l'=Length of hash function in our scheme.

Unit : ms

	T=100	T=200	T=300	T=400
n=10	120	151	165	182
n=20	220	237	242	280
n=30	320	327	339	370
n=40	420	450	462	510

(a)



(b)

Fig.2 The average time for Service Provider to Verify ring Sign, |N| = 352 bit

V. CONCLUSION AND FUTURE WORK

Motivated by the practical needs in data sharing, we proposed a new notion called Forward and Backward Secure ID-Based Ring Signature. It allows an ID-based ring signature scheme to have forward and backward security. It is the first in the literature to have this feature for ring signature in ID-based setting. Our scheme provides unconditional

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. 4, Issue 6, June 2016

anonymity and can be proven forward-secure unforgeable in the random oracle model, assuming RSA problem is hard. Our scheme is very efficient and does not require any pairing operations. The size of user secret key is just one integer, while the key update process only requires an exponentiation. We believe our scheme will be very useful in many other practical applications, especially to those require user privacy and authentication, such as ad-hoc network, e-commerce activities and smart grid. We consider a provably secure scheme with the same features in any cloud application as an open problem with detect various types of attack and how to handle those attack as future research work.

REFERENCES

1. X.Huang,J.K.Liu,S.Tang,Y.Xiang,K.Liang,L.Xu and J.Zhou,, "Cost Effective Authentic and Anonymous Data Sharing with Forward Security" , IEEE Transactions,Volume 64, 2015.
2. R.L.Rivest,A.Shamir,and Y.Tauman, " How to leak a Secret,volume" , LNCS 2248, pp. 552–565,2001.
3. R.Anderson, " Two remarks on public key cryptology " , ISSN 1476-2986 ,2002.
4. J.K.Liu and D.S.Wong, " Solutions to key exposure problem in ring signature " ,2008.
5. R.Gupta and Tanisha , " Enhanced Security for Cloud Storage using Hybrid Encryption", IJARCCE, Vol. 2, Issue 7,July 2013.
6. E.Abd,Al Latif,Al Badawi and A.Kayed,, "Enhancing the Data Security of the Cloud Computing Environment by Using Data Segregation Technique", 2015.
7. Subbiah,S.Selva and T.Ramkumar, " An Approach for Enhancing Secure Cloud Storage Using Vertical Partitioning Algorithm", Middle-East Journal of Scientific Research 23 (2): 223-230, 2015
8. P.Raut,V.Baporikar , " Design and Implementation of Enhanced Security in Multicloud Storage System Using Distributed File System", IJSETR, Volume 4, Issue 7, July 2015.
9. J.Yu,R.Hao,and F.Kong, "Forward secure identity-based signature", Information Sciences, Volume 181, Issue 3, Pages 648–660 , 1 February 2011
10. J.K.Liu,T.H.Yuen and J.Zhou,, "Forward secure ring signature without random oracles", 2011.
11. D.R.lin,C.I.Wang and D.J.Guan, " A Forward-Backward Secure Signature Scheme", Journal of Information Science and Engineering, 26(6):2319-2329,November 2010.
12 A.F.Sui,S.M.Yiu, " Separable and Anonymous Identity-Based Key Issuing " , ICPADS ,20-22 ,July 2005.
13. M.H.Au,J.K.Liu, "ID-Based Ring Signature Scheme" , Advances in Information and Computer Security, Volume 4266 of the series Lecture Notes in Computer Science pp 1-16, 2006.
14. R.Anderson " Two remarks on public-key cryptology" , Technical reports published by the University of Cambridge, ISSN 1476-2986, Dec 2000.
15 M.Bellare and S.Miner, " A forward-secure digital signature scheme " ,Lec notes in comp science, volume 1666,July 13 1999.

BIOGRAPHY

Pritee A.Raut recieved the BE degree in computer engineering from Savitribai Phule Pune University in 2013,now pursuing ME in computer engineering from Vishwabharati Academy's College of Engineering, Savitribai Phule Pune University, Ahmednagar, Maharashtra, India in 2015-16.