International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

# Cost-Effective Authentic and Anonymous Data Sharing With Forward Security

**T.SREEDHAR[1] & T.BABA[2]**
**[1]M-TECH, DEPT. OF CSE, P.V.K.K INSTITUTE OF TECHNOLOGY. ANANTHAPURAMU, AFFILIATED TO JNTUA, INDIA.**
**[2]ASSISTANT PROFESSOR, DEPT. OF CSE, P.V.K.K INSTITUTE OF TECHNOLOGY. ANANTHAPURAMU, AFFILIATED TO JNTUA, INDIA.**

**ABSTRACT**

Data sharing has never been more facile with the advances of cloud computing, and a precise analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a sizably voluminous number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an incognito and authentic data sharing system. It sanctions a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purport. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-predicated (ID-predicated) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-predicated ring signature by providing forward security. If a secret key of any utilizer has been compromised, all anterior engendered signatures that include this utilizer still remain valid. This property is especially paramount to any immensely colossal scale data sharing system, as it is infeasible to ask all data owners to re authenticate their data even if a secret key of one single utilizer has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

**Key words**: -Cloud Computing, Forward Security, Smart Grid, Data Distribution, Authentication , Ring Signature

## INTRODUCTION

Forward secure identity predicated ring signature for data sharing in the cloud provide secure data sharing within the group in an efficient manner. It additionally provides the authenticity and anonymity of the users. Ring signature is a promising candidate to construct an incognito and authentic data sharing system. It sanctions a data owner to surreptitiously authenticate his data which can be put into the cloud for storage or analysis purport. The system can be evade costly certificate verification in the traditional public key infrastructure setting becomes a bottleneck for this solution to be scalable. Identity-predicated ring signature which eliminates the process of certificate verification can be used instead. The security of ID-predicated ring signature by providing forward security: If a secret key of any utilizer has been rev, all precedent engendered signatures that include this utilizer still remain valid. The property is especially paramount to any immensely colossal scale data sharing system, as it is infeasible to ask all data owners to re-authenticate their data even if a secret key of one single utilizer has been conceded. Accountability and privacy issues regarding cloud are becoming a consequential barrier to the wide adoption of cloud accommodations. There is a plethora of advancement takes place in the system with veneration to the cyber world as a major concern in its implementation in a well efficacious manner respectively and additionally provide the system in multi-cloud environment. Many of the users are getting magnetized to this technology due to the accommodations involved in it followed by the reduced computation followed by the cost and additionally the reliable data transmission takes place in the system in a well efficacious manner respectively.

## 2. RELEGATED WORK

### 2.1Existing System

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.

The first ID-based ring signature scheme was proposed in 2002 which can be proven secure in the random oracle model. Two constructions in the standard model were proposed. Their first construction however

was discovered to be flawed, while the second construction is only proven secure in a weaker model, namely, selective-ID model. The first ID-based ring signature scheme claimed to be secure in the standard model is due to Han et al. under the trusted setup assumption. However, their proof is wrong and is pointed out.

**2.2Proposed System**

In this paper, we propose a new notion called forward secure ID-based ring signature, which is an essential tool for building cost-effective authentic and anonymous data sharing system. For the first time, we provide formal definitions on forward secure ID-based ring signatures. We present a concrete design of forward secure ID-based ring signature. No previous ID-based ring signature schemes in the literature have the property of forward security, and we are the first to provide this feature. We prove the security of the proposed scheme in the random oracle model, under the standard RSA assumption.

**3. IMPLEMENTATION**

**3.1 Verifier:**

•Verifier stores all the users and provides authorization.

•Verifier Authorize login for the user and stores all metadata.

•Verifier checks user login by group sign (username + address sign) and view all user registration with their sign.

•Verifier captures data modifiers.

**3.2Data Owner**

•Data owner has to register to verifier and Then verifier checks when data owner logins, user name must be unique.

•Data owner browse the file, and upload to the cloud server.

•Data owner generate file signature for the file he upload to the cloud server.

**3.3Cloud server**

•Cloud server receives all files from the data owner and store those files

•Cloud server checks the data integrity (Identification) in the cloud and inform to verifier.

•Cloud server maintains file transaction details and Calculate CPU Energy for each and every file uploads

**3.4 Receiver:**

Receiver Request secret key to download the file from cloud server and request for availability of files in the cloud server.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

## 4. EXPERIMENTAL RESULTS


**Fig 1 Registration form along with IP address**

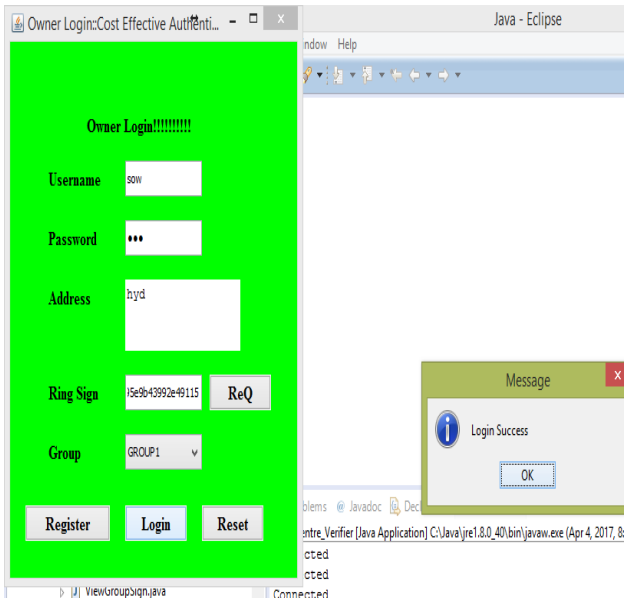


**fig 2 login form and status of login if all the details are correct.**

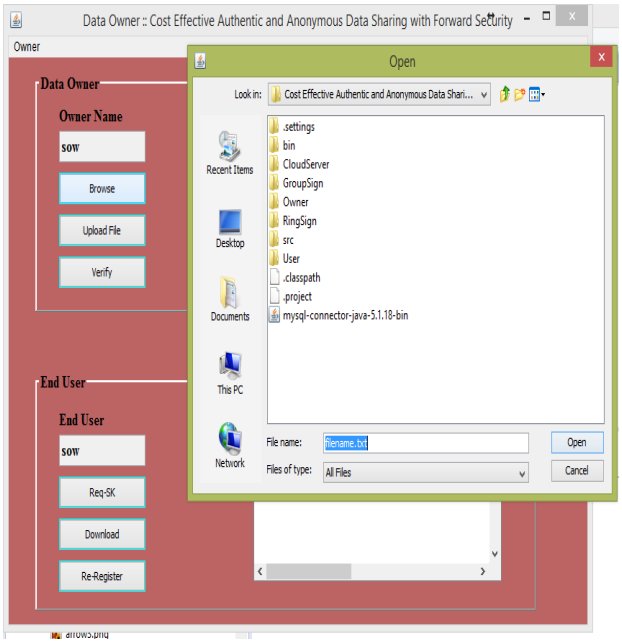


**Fig 3 To browse the file to upload into the cloud.**

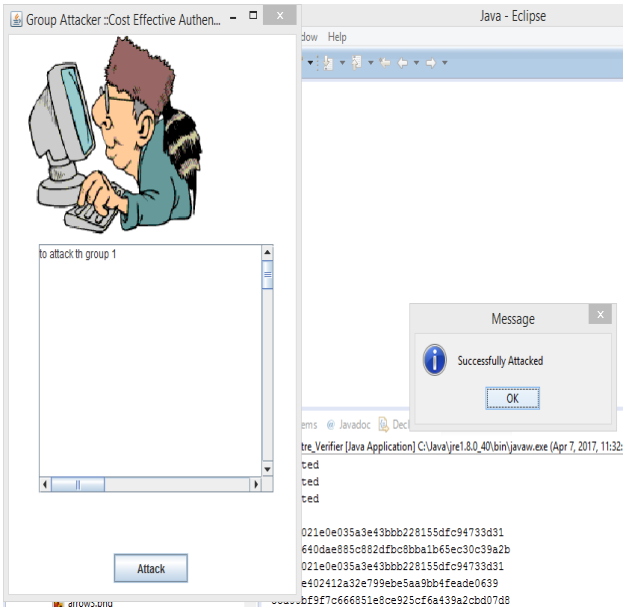


**Fig 4 Group attack and will be recovered automatically**

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

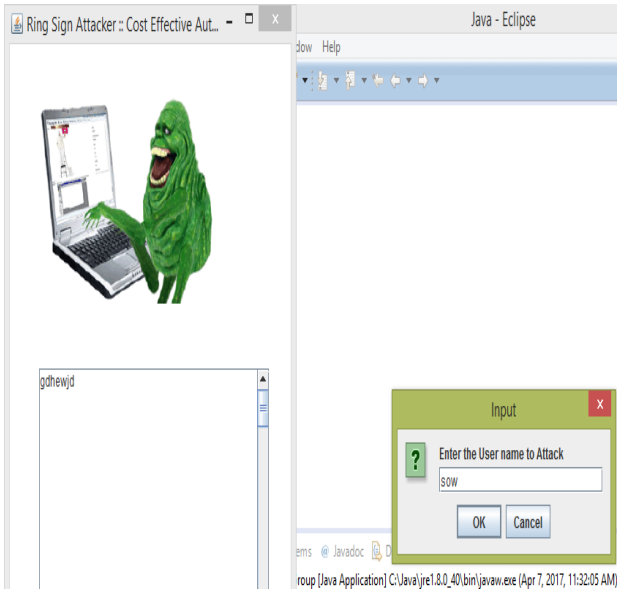


**Fig 6 Ring signature attack**

## 5. CONCLUSION

We proposed an incipient kinetics called forward secure ID-predicated ring signature. It sanctions an ID-predicated ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-predicated setting. Our orchestration gives unconditional obscurity and can be demonstrated forward-secure unforgivable in the desultory oracle model, expecting RSA issue is hard. Our scheme is very efficient and does not require any pairing operations. We believe our orchestration will be astronomically subsidiary in numerous other plausible practical applications, concretely to those require utilizer privacy, bulwark and validation, such as ad-hoc network, e-commerce activities and astute grid. Our present system depends on the arbitrary oracle to demonstrate its security. to ameliorate security for authentication on ring members utilizing MAC algorithm. SHA-1 and MD5 algorithm is utilized for data encryption. In this algorithm is utilized for sizably voluminous size of data should be encrypted. Sharing data on one ring members to another ring member. Then enhance security on data sharing and upload the data on cloud. We consider a provably secure scheme with the same features in the standard model as an open quandary and our future research work.

## 6. REFERENCE

[1] 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.

[2] R. Anderson. Two remarks on public-key cryptology. Manuscript, Sep. 2000. Relevant material presented by the author in an invited lecture at the Fourth ACM Conference on Computer and Communications Security, 1997.

[3] 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.

[4] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong. Id-based ring signature scheme secure in the standard model. In IWSEC, volume 4266 of Lecture Notes in Computer Science, pages 1–16. Springer, 2006.

[5] A. K. Awasthi and S. Lal. Id-based ring signature and proxy ring signature schemes from bilinear pairings. CoRR, abs/cs/0504097, 2005.

[6] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of group signatures: formal definitions, simplified requirements and a construction based on general assumptions. In EUROCRYPT'03, volume 2656 of Lecture Notes in Computer Science. Springer, 2003.

[7] M. Bellare and S. Miner. A forward-secure digital signature scheme. In Crypto'99, volume 1666 of Lecture Notes in Computer Science, 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., 10(4):212–224, 2013.

[9] A. Boldyreva. Efficient Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap Diffie-Hellman Group Signature Scheme. In PKC'03, volume 567 of Lecture Notes in Computer Science, pages 31–46. Springer, 2003.

[10] D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. In CRYPTO 2004, volume 3152 of Lecture Notes in Computer Science, pages 41–55. Springer, 2004.