# Forwardsecurity using ID-based Ring Authentication on data sharing in cloud

C.Indumathi [1]& Ms.M.Sharmila Devi [2]

[1]M-Tech,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

[2]Asst.Professor,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

**Abstract**: - Data sharing has never been easier with the advances of cloud computing, and an accurate analysis onthe shared data provides an array of benefits to both the society and individuals. Data sharing with a large number ofparticipants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ringsignature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data ownerto anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costlycertificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution tobe scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can beused instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: Ifa secret key of any user has been compromised, all previous generated signatures that include this user still remainvalid. This property is especially important to any large scale data sharing system, as itis impossible to ask all data owners to re-authenticate their data even if a secret key of one single user has beencompromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide animplementation to show its practicality.

Keywords: - ID-based Ring Signature, Authentication, data sharing in cloud, forward security.

## 1. INTRODUCTION

Forward secure character based ring signature for data sharing in the cloud provide secure data sharing of within the group in an efficient manner. It also provide of the authenticity and anonymity of the users. Ring signature is the promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to thein secret authenticate his data which can be put into the cloud for storage or analysis purpose. The system can be to avoid costly certificate verification in the traditional public key infrastructure setting becomes a bottleneck for this solution to be scalable. Identity-based ring the signature which is eliminates of the process of certificate for verification can be used instead. The security of the ID-based ring signature by providing forward security: If a secret key of any user has been revolution, all previous generated signatures that include this user still remain valid. The property is especially important to any large scale of data sharing system, as it is impossible to ask all data owners to re-authenticate their data even if a secret key of the one single user has been conceded. Accountability and privacy issues regarding cloud are becoming the significant barrier to the wide adoption of cloud services. There is the lot of advancement takes place in the system with respect to the internet as a major concern in it'simplementation in a well effective manner respectively and also provide of the system in multi-cloud environment. Many of the users are a getting attracted to this technology due to the services involved in it the followed by the reduced computation followed by the cost and also the reliable data of transmission takes place in the system in a well effective manner respectively.[9]

## 2. RELATED WORK

### Existing 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.

**Data Authenticity:** In the situation of smart grid, the statistic energy usage data would be misleading if it is forged by adversaries. While this issue alone can be solved using well established cryptographic tools (e.g., message authentication code or digital signatures), one may encounter additional difficulties when other issues are taken into account, such as anonymity and efficiency.

**Anonymity:** Energy usage data contains vast information of consumers, from which one can extract the number of persons in the home, the types of electric utilities used in a specific time period, etc. Thus, it is critical to protect the anonymity of consumers in such applications, and any failures to do so may lead to the reluctance from the consumers to share data with others.

### Proposed 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.Ring signature is a group-oriented signature with privacy protection on signature producer. A user can sign anonymously on behalf of a group on his own choice, while group members can be totally unaware of being conscripted in the group. Any verifier can be convinced that a message has been signed by one of the members in this group (also called the Rings), but the actual identity of the signer is hidden.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.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 (say, energy usage data sharing in smart-grid).

## 3. IMPLEMENTATION

**Sign:** On input a list param of system parameters, a time period $t$, a group size $n$ of length polynomial in $\lambda$, a set $L = \{IDi \in \{0, 1\}* | i \in [1, n]\}$ of $n$ user identities, a message $m \in M$, and a secret key $sk\pi,t \in D$, $\pi \in [1, n]$ for time period $t$, the algorithm outputs a signature $\sigma \in \Psi$.

**Verify:** On input a list param of system parameters,a time period $t$, a group size $n$ of length polynomial in $\lambda$, a set $L = \{IDi \in \{0, 1\}* | i \in [1, n]\}$ of $n$ user identities, a message $m \in M$, a signature $\sigma \in \Psi$, it outputs either valid or invalid.

**Update:** On input a user secret key $ski,t$for a time period $t$, the algorithm outputs a new user secret key $ski,t+1$ for the time period $t + 1$.

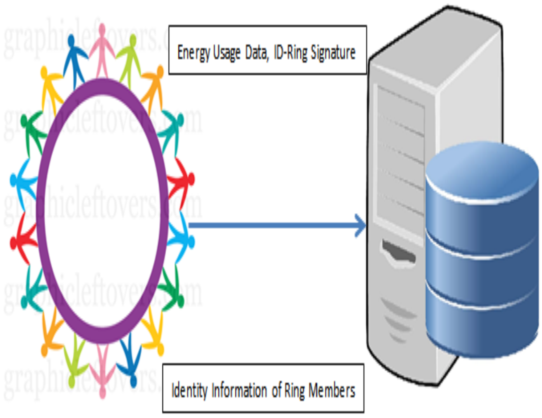
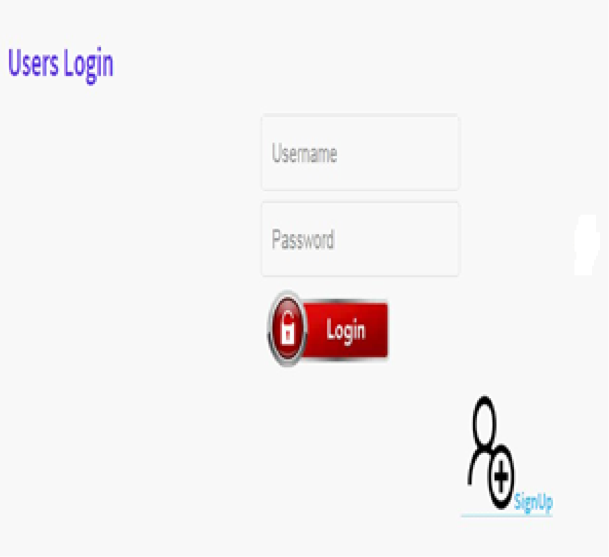

Energy Usage Data, ID-Ring Signature
Identity Information of Ring Members

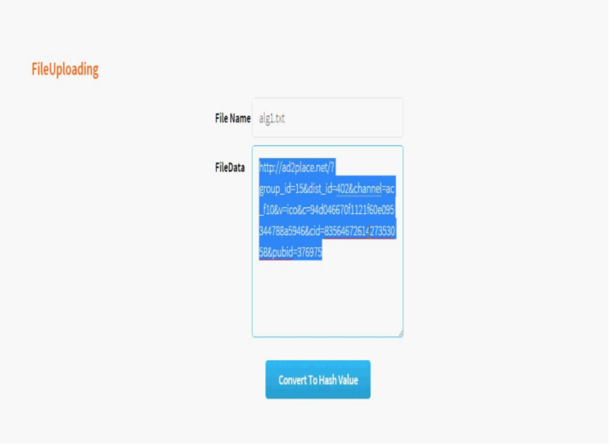
Fig: - 1 A Solution based on ID-based Ring Signature

## 4. EXPERIMENTAL RESULT



Users Login

Fig: 2 Authentications

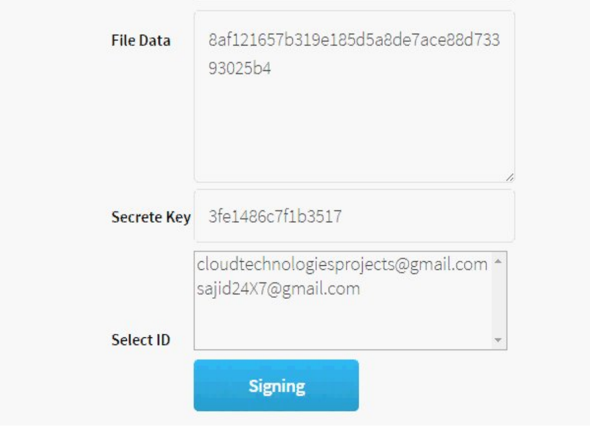


FileUploading

File Name alg1.txt

FileData http://ad2place.net/?group_id=15&dist_id=402&channel=ac_f10&v=ico&c=94d046670f1121f60e095344788a5946&cid=8356467261427353058&pubid=376975

Fig: 3 Data Upload in Cloud

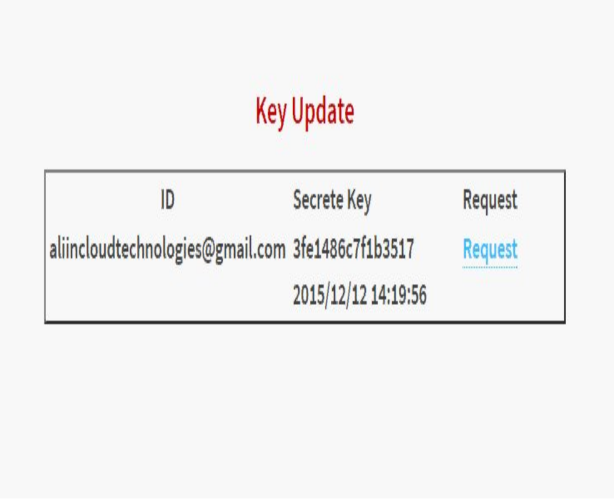


File Data 8af121657b319e185d5a8de7ace88d73393025b4

Secrete Key 3fe1486c7f1b3517

Select ID cloudtechnologiesprojects@gmail.com sajid24X7@gmail.com

Fig: 4 File Data Secrete Keys Generation



Key Update

| ID | Secrete Key | Request |
|---|---|---|
| aliincloudtechnologies@gmail.com | 3fe1486c7f1b3517<br>2015/12/12 14:19:56 | Request |

Fig: Request Sending

## 5. CONCLUSIONS

The Forward Secure ID-Predicated Ring Signature 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. The scheme provides unconditional anonymity and can be proven forward-secure unforgeable in the desultory oracle model. The scheme is very efficient and does not require any pairing operations. The size of utilizer secret key is just one integer, while the key update process only requires an exponentiation. This will be very utilizable in many other practical applications, especially to those require utilizer privacy and authentication, such as ad-hoc network, e-commerce activities and perspicacious grid. The system withal implemented in multi-cloud system to ameliorate the efficiency, sizably voluminous storage and data sharing system. Thus Reduce computation involution of designation and verify. Reduce space and time requisites ameliorate the cost efficient mechanism. The current scheme relies on the arbitrary oracle postulation to prove its security. Consider a provably secure scheme with the same features in the standard model as an open quandary and our future research work

## 6. REFERENCES

[1] Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou "Cost-effective authentic and anonymous data sharing withforward security".DOI:10.1109/TC.2014.2315619,IEEE Transactions on Computers.

[2] Javier Herranz IIIA, " Identity-Based Ring Signatures From RSA " Artificial Intelligence Research Institute, CSIC, Spanish National Research Council,Campus UAB s/n, E-08193 Bellaterra, Spain

[3] MihirBellare and Sara K. Miner" A Forward-Secure Digital Signature Scheme" Dept. of Computer Scienc e, &EngineeringUniversity of California at SanDiego, 9500 Gilman Drive La Jolla, CA 92093, USA.

[4] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, "Security And Privacy-Enhancing Multicloud Architectures" Member, IEEE,Luigi Lo Iacono.

[5] Gene ItkisBoston University Computer Science Dept.111 Cumming ton St.Boston, "Forward security: Adaptive cryptography-time evolution"MA 02215,USAitkis@bu.edu

[6] Y. Wu, Z. Wei, and R. H. Deng." Attribute-based access to scalable media in cloud-assisted content sharing networks" .IEEE Transactions on Multimedia,15(4):778–788, 2013.

[7] A. Shamir. "Identity-Based Cryptosystems and Signature Schemes".In CRYPTO 1984, volume 196 of Lecture Notes in Computer Science,pages 47–53.Springer, 1999.

[8] D. S. Wong, K. Fung, J. K. Liu, and V. K. Wei. “On the RS-CodeConstruction of Ring Signature Schemes and a Threshold Settingof RST”. In ICICS,volume 2836 of Lecture Notes in Computer Science,pages 34–46. Springer, 2003.

[9] 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 ofanonymity (extended abstract). In ProvSec, volume 6402 of Lecture Notes in Computer Science, pages 166–183. Springer, 2010.

[10] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen. Forward- secure identity-based signature: Security notions and construc- tion. Inf. Sci., 181(3):648–660, 2011.