International Journal For Technological Research In Engineering
Volume 5, Issue 10, June-2018 *ISSN (Online): 2347 - 4718*

EFFECTIVE AND AUTHENTIC DATA SHARING WITH FORWARD SECURITY

Sanjay Kumar Mathur
Assistant Professor, Department of Computer Science Engineering
Shekhawati Institute of Engineering and Technology, Sikar, Rajasthan, India

ABSTRACT: Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared dataprovides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into accountseveral issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to constructan anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be putinto the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI)setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the processof certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to reauthenticatetheir data even if a secret key of one single user has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

I. INTRODUCTION

The popularity and widespread use of "CLOUD" havebrought great convenience for data sharing and collection. Not only can individualsacquire useful data more easily, sharing data withothers can provide a number of benefits to our societyas well. As a representative example,consumers in Smart Grid can obtain their energyusage data in a fine-grained manner and are encouragedto share their personal energy usage data with others,e.g., by uploading the data to a third party platform suchas Microsoft Hohm (Fig. 1). From the collected dataa statistical report is created, and one can compare theirenergy consumption with others. This ability to access, analyze, and respond tomuch more precise and detailed data from all levels ofthe electric grid is critical to efficient energy usage.

Due to its openness, data sharing is always deployedin a hostile environment and vulnerable to a numberof security threats. Taking energy usage data sharingin Smart Grid as an example, there are several securitygoals a practical system must meet, including:

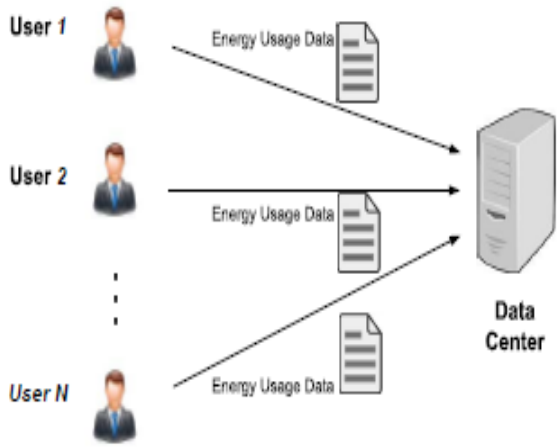

Fig. 1. Energy Usage Data Sharing in Smart Grid

Data Authenticity: In the situation of Smart Grid,the statistic energy usage data would be misleadingif it is forged by adversaries. While this issue alonecan be solved using well established cryptographictools (e.g., message authentication code or digitalsignatures), one may encounter additional difficultieswhen other issues are taken into account, suchas anonymity and efficiency;

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

Efficiency: The number of users in a data sharingsystem could be HUGE (imagine a smart grid witha country size), and a practical system must reduce the computation and communication cost as muchas possible. Otherwise it would lead to a waste ofenergy, which contradicts the goal of Smart Grid.

IMPLEMENTATION
MODULES:
Cloud Service Provider
Data Owner Module
ID-based ring signature
Efficiency Analysis

MODULES DESCRIPTION:

Cloud Service Provider

- In the first module, we develop the System model of Cloud with the Users.
- In this module, we develop Cloud Service Provider module. This is an entity that provides a data storage service in public cloud.
- The S-CSP provides the data outsourcing service and stores data on behalf of the users.
- In this paper, we assume that S-CSP is always online and has abundant storage capacity and computation power.
- And also it approves the group.

Data Owners Module

- A data owner is an entity that wants to outsource data storage to the S-CSP and access the data later.
- The Data owner uploads the file in the cloud.

ID-based ring signature

The energy data owner (say, Bob) first setups a ring by choosing a group of users. This phase only needs the public identity information of ring members, such as residential addresses, and Bob does not need the collaboration (or the consent) from any ring members.

Bob uploads his personal data of electronic usage, together with a ring signature and the identity information of all ring members.

By verifying the ring signature, one can be assured that the data is indeed given out by a valid resident (from the ring members) while cannot figure out who the resident is. Hence the anonymity of the data provider is ensured together with data authenticity. Meanwhile, the verification is efficient which does not involve any certificate verification.

Efficiency Analysis

- ID-based ring signature seems to be an optimal trade-off among efficiency, data authenticity and anonymity, and provides a sound solution on data sharing with a large number of participants.
- The size of public parameters is a constant, which only consists of some security parameters, two integers and some hash functions. The secret key is very short. It is only an integer. Assume we use 1,024-bit RSA security level, the secret key is just 1,024 bits.

II. 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.
- 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.

DISADVANTAGES OF EXISTING SYSTEM

- 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.
- Efficiency: The number of users in a data sharing system could be HUGE (imagine a smart grid with a country size), and a practical system must reduce the computation and communication cost as much as possible. Otherwise it would lead to a waste of energy, which contradicts the goal of smart grid.

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;
- We present a concrete design of forward secure IDbased 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

ADVANTAGES OF PROPOSED SYSTEM

- It is in ID-based setting. The elimination of the costly certificate verification process makes it scalable and especially suitable for big data analytic environment.
- The size of a secret key is just one integer.
- Key update process only requires an exponentiation.
- We do not require any pairing in any stage.

SCREENS

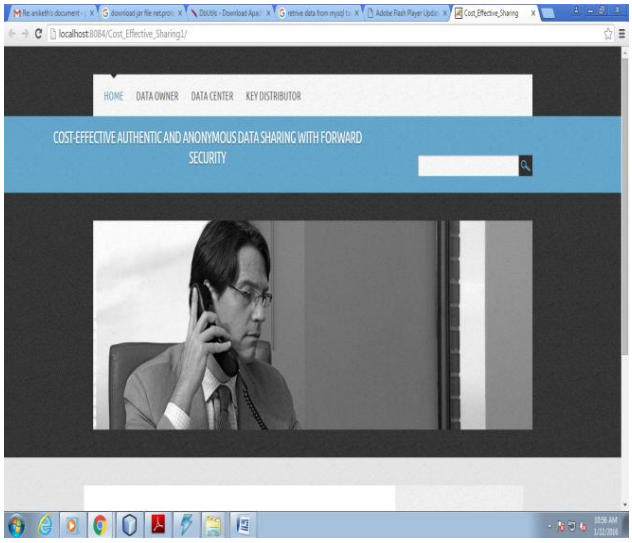

Fig: Home

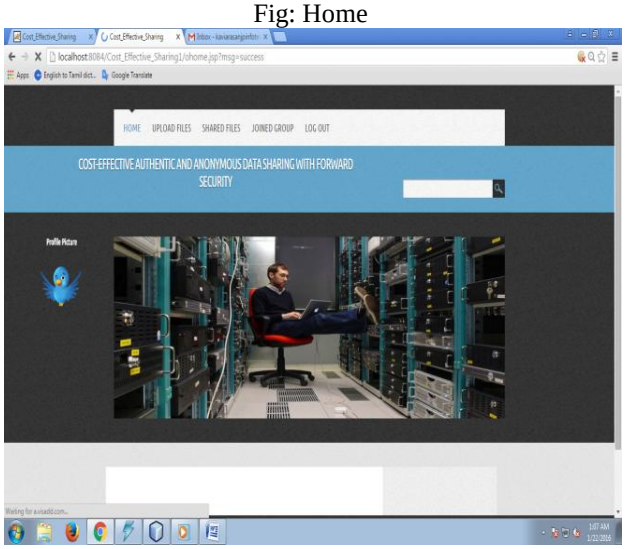

Fig: Owner Home

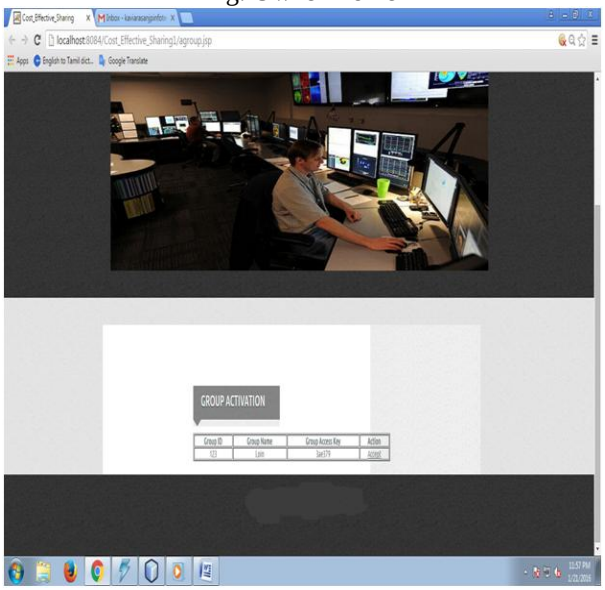

Fig: Group Activation

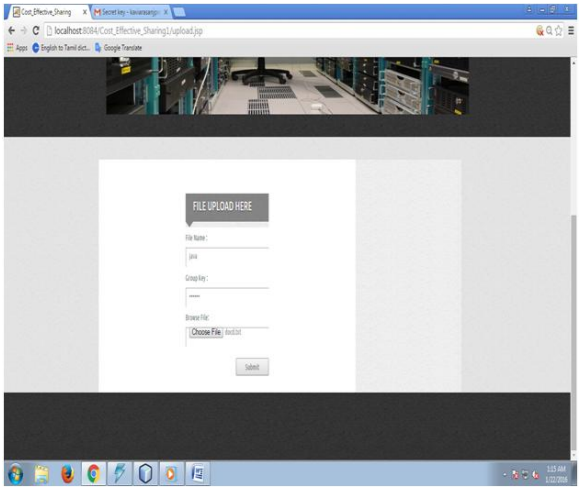

Fig: File Upload

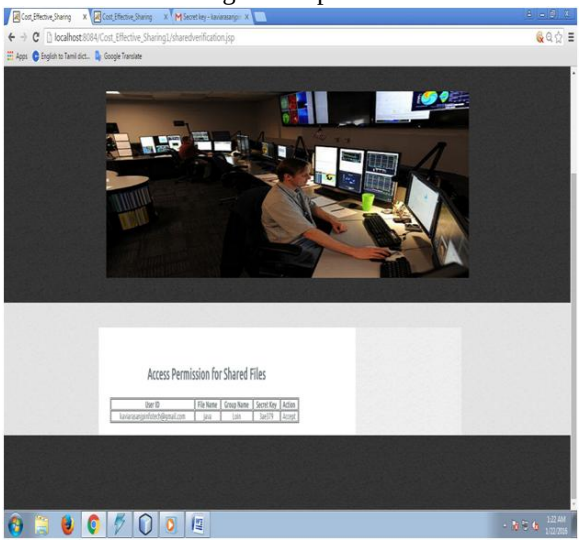

Fig: Access Permission

III. CONCLUSION

Motivated by the practical needs in data sharing, we proposed a new notion called forward secure ID-based ring signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-based setting. Our scheme provides unconditional 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. Our current scheme relies on the random oracle assumption to prove its security. We consider a provably secure scheme with the same features in the standard model as an open problem and our future research work.

REFERENCES

[1] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol., 2002, vol. 2501, pp. 415–432.

[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 Proc. 20th Annu. Int. Cryptol. Conf. Adv. Cryptol., 2000, vol. 1880, pp. 255–270.

[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 Proc. 1st Int. Workshop Security Adv. Inform. Comput. Security, 2006, vol. 4266, pp. 1–16.

[5] A. K. Awasthi and S. Lal, "Id-based ring signature and proxy ring signature schemes from bilinear pairings," CoRR, vol. 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 Proc. 22nd Int. Conf. Theory Appl. Cryptographic Techn., 2003, vol. 2656, pp. 614–629.

[7] M. Bellare and S. Miner, "A forward-secure digital signature scheme," in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, pp. 431–448.

[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] A. Boldyreva, "Efficient threshold signature, multisignature and blind signature schemes based on the gap Diffie-Hellman group signature scheme," in Proc. 6th Int. Workshop Theory Practice PublicKey Cryptography: Public Key Cryptography, 2003, vol. 567, pp. 31–46.

