

Cost-Effective Authentic and Anonymous Data Sharing with Forward Security

^[1] D.Malavika, ^[2] A.Amrutha, ^[3] N.Nalini, ^[4] Ms.D.Vinodha
^{[1][2][3]} U.G scholar ^[4] Assistant professor

^{[1][2][3][4]} Department of Computer Science and Engineering
S.A.Engineering College, Chennai (TN), India

^[1]malavika05061995@gmail.com ^[2]amrutha05091994@gmail.com ^[3]nalini181294@gmail.com,
^[4]vinodha@saec.ac.in

Abstract: Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large 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 anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into 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 process of 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 re-authenticate their 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.

Key words—Authentication, data sharing, cloud computing, forward security, smart grid.

I. INTRODUCTION

The popularity and widespread use of “CLOUD” have brought great convenience for data sharing and collection. Not only can individuals acquire useful data more easily, sharing data with others can provide a number of benefits to our society as well. As a representative example, consumers in Smart Grid can obtain their energy usage data in a fine-grained manner and are encouraged to share their personal energy usage data with others, e.g., by uploading the data to a third party platform such as Microsoft Hohm (Fig. 1). From the collected data a statistical report is created, and one can compare their energy consumption with others. This ability to access, analyze, and respond to much more precise and detailed data from all levels of the electric grid is critical to efficient energy usage. Due to its openness, data sharing is always deployed in a hostile environment and vulnerable to a number of security threats. Taking energy usage data sharing in Smart Grid as an example, there are several security goals a practical system must meet, including: 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), 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, 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.

This paper is devoted to investigating fundamental security tools for realizing the three properties we described. Note that there are other security issues in a data sharing system which are equally important, such as availability and access control.

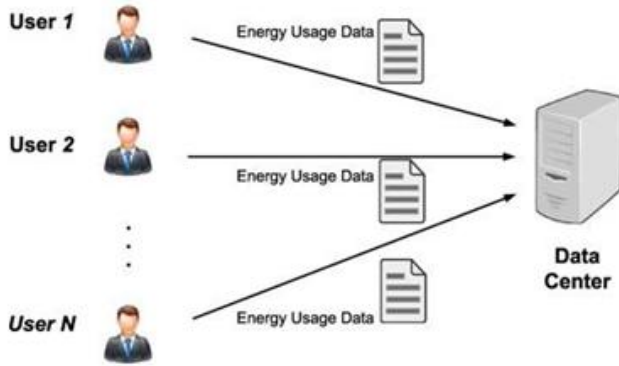


Fig. 1. Energy usage data sharing in smart grid.

A. Identity-Based Ring Signature

The aforementioned three issues remind us a cryptographic primitive “identity-based ring signature”, an efficient solution on applications requiring data authenticity and anonymity.

B. ID-Based Cryptosystem

Identity-based (ID-based) cryptosystem, introduced by Shamir [45], eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming. 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. This property avoids the need of certificates (which are necessary in traditional public-key infrastructure) and associates an implicit public key (user identity) to each user within the system. 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).

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. Ring signatures could be used for whistle blowing, anonymous membership authentication for ad hoc groups and many other applications which do not want complicated group formation stage but require signer anonymity. There have been many different schemes proposed since the first

appearance of ring signature in 1994 and the formal introduction in 2001.

C. An Affirmative Advantage in Big Data

Due to its natural framework, ring signature in ID-based setting has a significant advantage over its counterpart in traditional public key setting, especially in the big data analytic environment. Suppose there are 10,000 users in the ring, the verifier of a traditional public key based ring signature must first validate 10,000 certificates of the corresponding users, after which one can carry out the actual verification on the message and signature pair. In contrast, to verify an ID-based ring signature, only the identities of ring users, together with the pair of message and signature are needed. As one can see, the elimination of certificate validation, which is a costly process, saves a great amount of time and computation. This saving will be more critical if a higher level of anonymity is needed by increasing the number of users in the ring. Thus, as depicted in Fig. 2, ID-based ring signature is more preferable in the setting with a large number of users such as energy data sharing in smart grid:

Step 1: 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.

Step 2: Bob uploads his personal data of electronic usage, together with a ring signature and the identity information of all ring members.

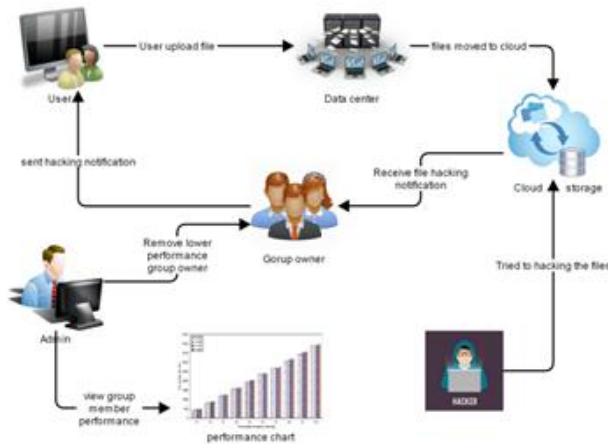
Step 3: By verifying the ring signature, one can be assured that the data is indeed given out by a valid resident (from the ring members) while cannot figure out who the resident is. Hence the anonymity of the data provider is ensured together with data authenticity. Meanwhile, the verification is efficient which does not involve any certificate verification. The first ID-based ring signature scheme was proposed.

II. OUR PROPOSED ID-BASED RING SIGNATURE SCHEME

Data sharing with a large 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 anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into 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 process of certificate verification, can be used instead. In

this project, 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 reauthenticate their 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.

Fig. 2. Proposed Architecture Ring Signature Based.



III. MODULE DESCRIPTION

a) Authentication:

Authentication is the act of confirming the truth of an attribute of a single piece of data (datum) or entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity.

b) Data sharing:

Data sharing is the practice of making data used for scholarly research available to other investigators. Replication has a long history in science. Many funding agencies, institutions, and publication venues have policies regarding data sharing because transparency and openness are considered by many to be part of the scientific method.

c) Cloud Computing.

Cloud computing is a computing term or metaphor that evolved in the late 2000s, based on utility and consumption of computer resources. Cloud computing involves deploying groups of remote servers and software networks that allow different kinds of data sources be uploaded for real time processing to generate computing results without the need to store processed data on the cloud.

d) Identity-based Ring Signature

Private or hybrid Identity-based (ID-based) crypto system introduced and eliminated the need for verifying the

validity of public key certificates, the management of which is both time and cost consuming. In an ID based crypto system, the public key of each user is easily comparable from a string corresponding to this user's publicly known identity (e.g., an email address, a residential address, etc.).

e) Forward security

In cryptography, forward secrecy (FS; also known as perfect forward secrecy, or PFS) is a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. Even worse, the "group" can be defined by the adversary at will due to the spontaneity property of ring signature: The adversary only needs to include the compromised user in the "group" of his choice.

f) Anonymous user:

A smart grid is a modernized electrical grid that uses analog or digital information and communications technology to gather and act on information - such as information about the behaviors of suppliers and consumers - in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the We implement the Smart Grid for user access.

A. DATA BASE

A database is a collection of interrelated data stored with minimum redundancy to serve many users quickly and efficiently. The general Objectives of the database design are to make the data access easy, inexpensive and flexible to the user. The data in the system has to be stored and retrieved from database.

Designing the database is the part of system design. Data elements and data structures to be stored have been identified at analysis stage and are structured and put together to design the data storage and retrieval system.

Field	Type	Constraints	Description
<i>id</i>	int(11)	Primary Key	Order Id
Reg_name	varchar(50)		Name of the user
Reg_Email	varchar(30)		Mail id of the user
Reg_password	varchar(20)		Password of the user
Reg_mobile	bigint(10)		Contact Number of the user

Reg_Location	int(11)		Location of user
Reg_date	varchar(30)		Registration date

Fig. 3. User Structure Data Base.

Field	Type	Constraints	Description
<i>p_id</i>	int(11)	Primary Key	Order Id
pro_name	varchar(50)		Name of the Provider
pro_Email	varchar(30)		Mail id of the Provider
pro_phone	bigint(10)		Contact Number of the Provider
address	varchar(30)		Location of Provider
date	varchar(80)		Registration date



Fig. 4. Provider Structure Data Base.

IV. APPLICATIONS OF ID-BASED RING SIGNATURES

WHISTLEBLOWING. Suppose Bob is a member of the city council. One day he wishes to leak secret news from the council meeting to a journalist. The news is supposed to be kept secret. Thus Bob wants to remain anonymous, yet such that the journalist is convinced that the leak was indeed from a council member. Bob cannot send to the journalist a standard digitally signed message, since such a message, although it convinces the journalist that it came from a council member, does so by directly revealing Bob's identity. Neither does it work for Bob to send the journalist a message through a standard anonymizer, since the anonymizer strips off all source identification and authentication in a way that the journalist would have no reason to believe that the message really came from a council member at all. Using another primitive called group signature does not solve the problem neither. A group

signature allows a signer to sign a message on behalf of a group. The verifier only knows that one of the users of the group signs the message yet does not know who the actual signer is. It does not work in this case, because it requires prior cooperation of the other group member to set up, and leaves Bob vulnerable to later identification by the group manager, who may be controlled by the government. The correct approach for Bob is to send the secret information to the journalist through an anonymizer, signed with a ring signature that names each council member including himself as a ring member. The journalist can verify the ring signature on the message, and learn that it definitely came from a council member. However, neither he nor anyone (including those council members inside the ring) can determine the actual source of the leak.

Forward security enhances the protection of all entities. Without forward security, if a secret key of a council member Alice is exposed, every ring signature containing Alice in the ring will become invalid. That means any previous ring signature given by Bob will be invalid (assuming Alice is included in the signature). This will greatly affect the accuracy of the report by the journalist who may rely on Bob for leaking important secret information.

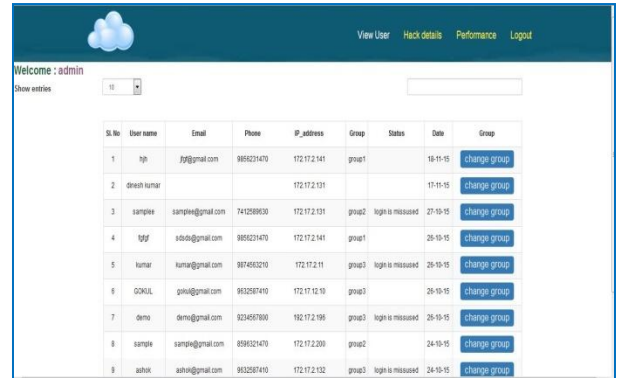
E-contract Signing. A 1-out-of-2 ring signature (containing two users in the ring) can be used to construct concurrent signature. A concurrent signature allows two entities to produce two signatures in such a way that, from the point of view of any third party, both signatures are ambiguous with respect to the identity of the signing party until an extra piece of information (the keystone) is released by one of the parties. Upon release of the keystone, both signatures become binding to their true signers concurrently.

Concurrent signature is one of the essential tools for building e-contract signing and fair exchange protocol in the paradigm. It can protect both parties against a cheating party. Consider the following example of fair tendering of contracts. Suppose that A has a building construction contract that she wishes to put out to tender, and suppose companies B and C wish to put in proposals to win the contract. This process is sometimes open to abuse by A since she can privately show B's signed proposal to C to enable C to better the proposal. Using concurrent signatures, B would sign his proposal to construct the building for an amount X, but keep the keystone private. If A wishes to accept the proposal, she returns a payment instruction to pay B amount X. She knows that if B attempts to collect the payment, then A will obtain the keystone through the banking system to allow the public to verify that the signature is really generated by B. But A may also wish to examine C's proposal before deciding which to accept. However there is no advantage for A to show B's signature to C since at this point B's signature is ambiguous and so C will not be convinced of anything at all by seeing it. We see that the

tendering process is immune to abuse by A.

Adding forward security to it can further improve the security protection level. With forward security, the key exposure of either party does not affect the e-contracts previously signed. This provides a more fair, justice, safety and efficient environment for commercial users doing business in an e-commerce platform.

E-auction. Similar to e-contract signing, ring signature schemes can be used to construct e-auction protocols. By using ring signature, a winner-identifiable anonymous auction protocol can be build efficiently. That is to say, the auctioneer can authenticate the real identity of the winner at the end of the protocol without additional interactions with the winning bidder even though all the bidders bid anonymously. Adding forward security further provides additional security to all entities involved in the auction activity. The loss of secret key by anybody does not affect the overall result.



Welcome : admin

Sl.No	User name	Email	Phone	IP_address	Group	Status	Date	Group
1	hpn	hpn@gmail.com	999523470	172.17.2.141	group1		19-10-15	change group
2	dinesh kumar			172.17.2.131			13-10-15	change group
3	sample	sample@gmail.com	741258930	172.17.2.151	group2	login is missused	27-10-15	change group
4	kgf	kgf@gmail.com	999523470	172.17.2.141	group1		25-10-15	change group
5	kumar	kumar@gmail.com	987456320	172.17.2.111	group3	login is missused	25-10-15	change group
6	GOKUL	goku@gmail.com	993256740	172.17.12.10	group3		25-10-15	change group
7	demo	demo@gmail.com	923456780	192.17.2.199	group3	login is missused	25-10-15	change group
8	sample	sample@gmail.com	8595321470	172.17.2.200	group2		24-10-15	change group
9	satish	satish@gmail.com	993256740	172.17.2.132	group3	login is missused	24-10-15	change group

Fig. 6. Provider Data Base in Cloud Computing



Welcome : Renu

Sl.No	File Name	File Size(KB)	File Type	File Id	File upload path IP	Name	Download
1	test.html	196	text/html	trcm			Download
2	sublime_text.exe	0		wfkg			Download
3	changeip.txt	20564	text/plain	y954	172.17.2.141		Download
4	0th review.doc	286269	application/zip	w157	172.17.2.141		Download

Fig. 7. User Data Base in Cloud Computing

V. RESULTS

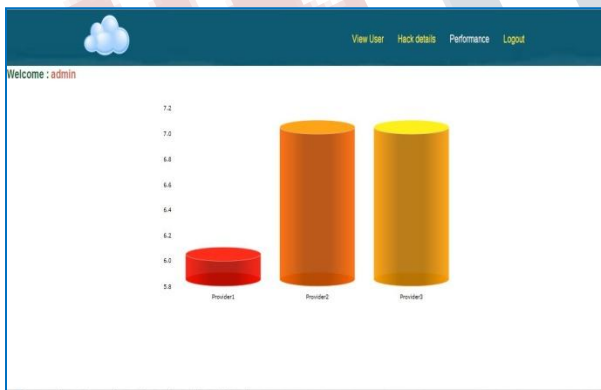


Fig. 5. Provider Usage in Cloud Computing

VI. CONCLUSION AND FUTURE ENHANCEMENT

We concluded that 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 unforgivable 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.

In this Paper ,we have added all the future, in further future enhancement for the design or developing the android app .Because all the user cant access the web services at any time. If the android app will come ,that will be act as eco friendly for the user.

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, 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,
- [7] M. Bellare and S. Miner, "A forward-secure digital signature scheme," in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, 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.
- [10] Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. Annu. Int. Cryptol. Conf. Adv. Cryptol., 2004, vol. 3152, pp. 41–55.
- [11] Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in Proc. 22nd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2002, vol. 2442, pp. 465–480.
- [12] J. Camenisch, "Efficient and generalized group signatures," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1997, vol. 1233, 465–479.
- [13] N. Chandran, J. Groth, and A. Sahai, "Ring signatures of sub-linear size without random oracles," in Proc. 34th Int. Colloq. Automata, Lang. Programming, 2007, vol. 4596, pp. 423–434.
- [14] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," IEEE Trans. Serv. Comput., vol. 5, no. 4, pp. 551–563, Fourth Quarter 2012.
- [15] D. Chaum and E. van Heyst, "Group signatures," in Proc. Work-shop Theory Appl. Cryptographic Techn., 1991, vol. 547, pp. 257–265.
- [16] L. Chen, C. Kudla, and K. G. Paterson, "Concurrent signatures," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, vol. 3027.
- [17] S. S. M. Chow, V.K.-W. Wei, J. K. Liu, and T. H. Yuen, "Ring signatures without random oracles," in Proc. ACM Symp. Inform., Comput., Commun. Security, 2006, pp. 297–302.
- [18] S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui, "Efficient identity based ring signature," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Security, 2005, vol. 3531, pp. 499–512.
- [19] R. Cramer, I. Damgard, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in Proc. 14th Annu. Int. Cryptol. Conf. Adv. Cryptol., 1994, vol. 839, 174–187.
- [20] R. Cramer and V. Shoup, "Signature schemes based on the strong RSA assumption," in Proc. ACM Conf. Comput. Commun. Security, 1999, pp. 46–51.
- [21] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in Ad Hoc groups," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, vol. 3027, pp. 609–626.
- [22] J. Han, Q. Xu, and G. Chen, "Efficient ID-based threshold ring signature scheme," in Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput., 2008, pp. 437–442.