ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Effective privacy policy and Anonymous Data Sharing with Forward Security

Ganta Swetha
Assitsant Professor
Department of IT
Teegala Krishna Reddy Engineeging College,
Medbowli, Medbowli, Saroornagar, Hyderabad.

O.Nagakumari
Assitsant Professor
Department of IT
Teegala Krishna Reddy Engineeging College,
Medbowli, Medbowli, Saroornagar, Hyderabad

ABSTRACT

Data sharing with a huge numeral of accomplices requisite take into account a number of concerns, including data owner's efficiency, data integrity and privacy. Ring signature is an auspicious candidate to build an unspecified and trustworthy data sharing system. It endures a data owner to anonymously endorse data which can be positioned into the cloud for storage or analysis determination.

The exorbitant certificate verification in the traditional public key infrastructure (PKI) setting suits a blockage for this elucidation to be ascendable. Identity-based (ID-based) ring signature, which eradicates the process of certificate verification, can be used instead. Data sharing has certainly not been tranquil with the progresses of cloud computing, and a precise analysis on the shared data runs an array of assistances to both the society and individuals. In this Improving efficiency, data integrity and Effective privacy policy and Anonymous Data Sharing with Forward Security, it is additionally enriched the security of ID-based ring signature by providing forward security.

Keywords-Authentication, data sharing, cloud computing, forward security, smart grid.

I.INTRODUCTION

The reputation and prevalent routine of "CLOUD" have fetched pronounced accessi bility for data sharing and collection [1]. The individuals can acquire useful data more easily as well as sharing data with others can provide a number of benefits to the society also. As a representative example, consumers in Smart Grid [4] can acquire their energy norm data in a fine-grained method and are stimulated to stake their personal energy usage data with others, like by uploading the data to a third party platform such as Microsoft Home. Starting the collected data a statistical report is formed, and one can equate their n energy consumption with others. This capacity to access, analyze, and return to much more precise and exhaustive data from all levels of the electric grid is critical to resourceful energy process. Due to its openness, data sharing is always organized in a hostile environment and vulnerable to a number of security threats. Taking energy usage data distribution in Smart Grid as an example, there are several security goals a practical system must meet, together with 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 recognized cryptographic tools, one may meet additional difficulties when other issues are taken into account, such as obscurity and proficiency.

Anonymity: Energy usage data contains vast information of consumers, from which one can citation 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; and 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. Else it would

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

lead to a waste of energy, which contradicts the goal of smart grid.

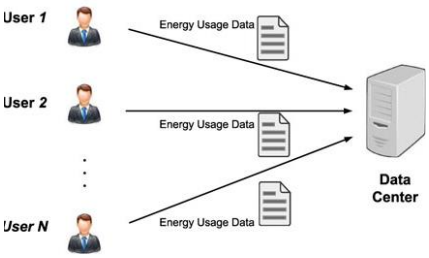


Fig 1. Energy usage data sharing in smart grid.

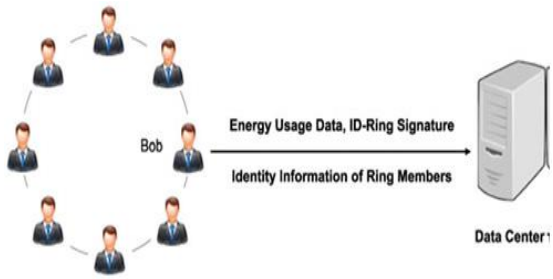


Fig 2. A solution based on ID-based ring signature.

1.1 IDENTITY-BASED RING SIGNATU RE:

The above-mentioned concepts remind a cryptographic primitive "identity-based ring signature", an efficient solution on applicati ons requiring data authenticity and anonymity.

1.2 ID-BASED CRYPTOSYSTEM:

Identity-based (ID-based) cryptosystem, introduced by Shamir [5], 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). The first ID-based ring signature scheme was proposed in 2002 [57] which can be proven secure in the random oracle model. Two constructions in the standard model were proposed in [4]. Their first construction however was discovered to be flawed [4], 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. [5] under the trusted setup assumption.

II.BACKGROUND AND RELATED WORK:

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. To obtain a higher level protection, one can add more users in the ring. But doing this increases the chance of key exposure as well.[9] Key exposure is the fundamental limitation of ordinary digital signatures. If the private key of a signer is compromised, all signatures of that signer become worthless: future signatures are invalidated and no previously issued signature can be trusted [10]. Once a key leakage is identified, key revocation mechanisms must be invoked immediately in order to prevent the generation of any signature using the compr omised secret key. However, this does not solve the problem of forge ability for past signatures.[11]The notion of forward secure signature was proposed to preserve the validity of past signatures even if the current secret key is compromised. The concept was first sugge sted by Anderson [2], and the solutions were designed by Bell are and Miner [7]. The idea is dividing the total time of the validity of a public key into T time periods, and a key compromise of the current time slot does not enable an adversary to produce valid signatur es pertaining to past time slots.[9]

2.1 KEY EXPOSURE IN BIG DATA SHARING SYSTEM:

The issue of key exposure is more severe in a ring signature scheme: if a ring member's secret key is

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

exposed, the adversary can produce valid ring signatures of any documents on behalf of that group. 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. As a result, the exposure of one user's secret key renders all previously obtained ring signatures invalid (if that user is one of the ring members), since one cannot distinguish whether a ring signature is generated prior to the key exposure or by which user. Therefore, forward security is a necessary requirement that a big data sharing system must meet. Otherwise, it will lead to a huge waste of time and resource.[10]While there are various designs of forward-secure digital signatures [4] adding forward security on ring signatures turns out to be difficult. As far as the authors know, there are only two forward secure ring signature schemes [5], [6]. However, they are both in the traditional public key setting where signature verification involves expensive certificate check for every ring member. This is far below satisfactory if the size of the ring is huge, such as the users of a smart grid. To summarize, the design of ID-based ring signature with forward security, which is the fundamental tool for realizing cost-effective authentic and anonymous data sharing, is still an open problem. In this improving efficiency, data integrity and effective privacy policy and anonymous data sharing with forward security, 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 is projected. For the first time, we provide formal definitions on forward secure ID-based ring signatures; A concrete design of forward secure ID-based ring signature is presented. 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; the security of the proposed scheme in the random oracle model, under the standard RSA assumption is proved. The practical implementation can be done in following ways: They are 1) 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.2) The size of a secret key is just one integer.3) Key update process only requires anexponentiation.4) We do not require any pairing in any stage.

III.PROPOSED SYSTEM: ID-BASED FO RWARD SECURING SIGNATURE SCHE ME:

Projected scheme involves the exponent e larger than 2, where 'e' is the bit length of the hash function H2. Frequently a secure hash function requires at least 160 bits output. However, if we set 160 it will be quite inefficient. In order to offset this, we can use different hash functions such that each hash function outputs '0 bits .We are supposed to reiterate the signing and verification procedures 8 times for each time using a different hash function H2 in order to achieve 160-bit hash function security. 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 and only an integer. Let us assume to use 1,024-bit RSA security level, the secret key is just 1,024 bits. For every key update process, it just requires an exponentiation with exponent e over modulus N operation. The signing and verification algorithms do not require any pairing operation. The computation complexity and space requirement of this scheme are shown in below table respectively.

3.1 COMPARING THE PROPOSED SCHEME WITH RELATED WORKS:

While comparing it is noticed that the verifica tion for non ID-based forward secure ring signature schemes entail an additional certif. icate verification for n users. We eradicate the cost and space for those n certificates substant iation in this assessment, as it might diverge in different circumstances.

IV.IMPLEMENTATION AND EXPER IMENTAL RESULTS:

Here it is implemented the smart grid example and evaluated the performance of ID-Based Forward Secure Ring Signature Scheme with respect to three entities: the private key generator, the energy data owner (user), and the service provider. In the experiments, the programs for three entities are implemented using the public cryptographic library MIRACL [14], programmed in C++. All experiments were repeatedly conducted to obtain average results

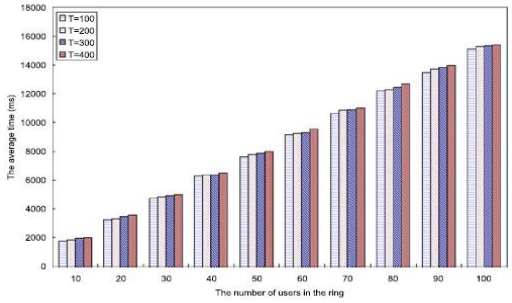
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

shown in this Improving efficiency, data integrity and Effective privacy policy and Anonymous Data Sharing with Forward Security.

The average time for the PKG to setup the system is shown in below Table respectively.

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



(Unit: ms)

	T=100	T=200	T=300	T=400
n=10	1763	1841	1950	1981
n=20	3261	3323	3464	3557
n=30	4727	4851	4930	4992
n=40	6271	6365	6380	6505
n=50	7628	7769	7846	8003
n=60	9173	9250	9297	9547
n=70	10623	10858	10889	10998
n=80	12184	12293	12449	12667
n=90	13479	13697	13853	13978
n=100	15116	15272	15319	15382

Parameters: $|N| = 2048$, $|k| = 1024$, $|\ell| = 320$.

V.CONCLUSION:

A new conception called forward secure ID-based ring signature allows an ID-based ring signature scheme to have forward security. It is the first in the literature to obligate this facility for ring signature in ID-based setting. This scheme provides unconditional anonymity and can be proven forward-secure unforgettable in the random oracle model, supposing RSA problem is durable. This scheme is very effective and does not necessitate any coupling processes. The size of user secret key is just one integer, while the key upgrade process only requires an exponentiation. We believe our scheme will be very useful in many other hands-on applications, particularly to those which entail user privacy and authentication, such as ad-hoc network, e-commerce accomplishments and smart grid. The current scheme depends on the random oracle supposition to attest its security.

REFERENCES

[1] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from avariety 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 aninvited lecture at the Fourth ACM Conference on Computer andCommunications Security, 1997.)

[3] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practicaland 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 ringsignature 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 ofgroup signatures: Formal definitions, simplify ied requirements and a construc tion 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 signaturescheme," 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,"

IEEETrans. Dependable Sec. Comput., vol. 10, no. 4, pp. 212–224, Jul.\Aug. 2013.

[9] A. Boldyreva, "Efficient threshold signature, multisignatureand blind signature schemes based on the gap Diffie-Hellmangroup signature scheme," in Proc. 6th Int. Workshop TheoryPractice PublicKey Cryptograp hy: Public Key Cryptography, 2003,vol. 567, pp. 31–46.

[10] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," inProc.Annu. Int . Cryptol. Conf. Adv. Cryptol., 2004, vol. 3152, pp. 41–55.

[11] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signaturesand 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," inProc. Int. Conf. Theory Appl. Cryptographic Techn., 1997, vol. 1233,pp. 465–479.

[13] N. Chandran, J. Groth, and A. Sahai, "Ring signatures of sublinearsize without random oracles," in Proc. 34th Int. Colloq.Automata, Lang. Programm ing, 2007, vol. 4596, pp. 423–434.

[14] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: Avision for socially motivated resource sharing," IEEETrans.Serv.Comput.,vol.5,no.4,pp.551–563,FourthQuarter2012.

[15] D. Chaum and E. van Heyst, "Group signatures," in Proc. WorkshopTheory 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,pp. 287–305