Cost Effective and Authoritative Send Anonymous Data Safely Forward

[1]SUDINI PRIYANKA [2]V RAMA RAO

[1] PG Scholar , Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206.

[2]Assistant Professor, Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206

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.

1 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 (e.g., from the same block).

2 SECURITY MODEL

A ð1; nÞ ID-based forward secure ring signature (IDFSRS) scheme is a tuple of probabilistic polynomial-time (PPT) algorithms: Setup. On input an unary string 1_ where _ is a security parameter, the algorithm outputs a master secret key msk for the third party private key generator and a list of system parameters param that includes and the descriptions of a user secret key space D, a message spaceMas well as a signature space C. Extract. On input a list param of system parameters, an identity IDi 2 f0; 1g_ for a user and the master secret key msk, the algorithm outputs the user's secret key ski;0 2 D such that the secret key is valid for time t ¼ 0. In this paper, we denote time as nonnegative integers. When we say identity Idi corresponds

to user secret key ski;0 or vice versa, we mean the pair ðIDi; ski;0Þ is an input-output pair of Extract with respect to param and msk. _ Update. On input a user secret key ski;t for a time period t, the algorithm outputs a new user secret key ski;tþ1 for the time period t þ 1Verify. On input a list param of system parameters, a time period t, a group size n of length polynomial in _, a set L ¼ fIDi 2 f0; 1g_ji 2 ½1; n_g of n user identities, a message m2M, a signature s 2 C, it outputs either valid or invalid. Correctness. A ð1; nÞ IDFSRS scheme should satisfy the verification correctness—signatures signed by honest signer are verified to be invalid with negligible probability.

3 OUR PROPOSED ID-BASED FORWARDSECURERING SIGNATURE SCHEME

This section is devoted to the description and analysis of our proposed ID-based forward secure ring signature scheme.

3.1 The Design

We assume that the identities and user secret keys are valid into T periods and makes the time intervals public. We also set the message spaceM ¼ f0; 1g_.Setup. On input of a security parameter _, the PKG generates two random k-bit prime numbers p and q such that p ¼ 2p0 þ 1 and q ¼ 2q0 þ 1 where p0; q0 are some primes. It computes N ¼ pq. For some fixed parameter ', it chooses a random prime number e such that 2' < e < 2'þ1 and gcdðe; fðNÞÞ ¼ 1. It chooses two hash functions H1 : f0; 1g_ ! Z_N andH2 : f0; 1g_ ! f0; 1g'. The public parameters param are ðk; '; e; N;H1;H2Þ and the master secret key msk is ðp; qÞ Extract. For user i, where i 2 Z, with identity IDi 2 f0; 1g_ requests for a secret key at time period t (denoted by an integer), where 0 _ t < T, the PKG computes the user secret key

mod N

4 .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.

5 .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;

6. MAIN MODULES

User Module In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

Distributed Clustering

The Distributional clustering has been used to cluster words into groups based either on their participation in particular grammatical relations with other words by Pereira et al. or on the distribution of class labels associated with each word by Baker and McCallum .

7.DESIGN

Input design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. **.**

System testing

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner.

Implementation Datawoner

In this module, data owner has to register to verifier and when verifier checks when data owner login , user name must be unique. Data owner browse the file , encrypt and upload file with its mac. Data owner generate sign (mac) based on username and address while registration. Data owner generate group sign. Data owner verify the data from verifier.

Verifier

In this module verifier checks user login by group sign (username + address sign) and view all user registration with their sign. verifier list all users and provide authorization and authorize only valid users. Authorize login for the user and stores all metadata and Verifier capture data modifiers.

Data centre

Maintain all transaction record (upload and download)

8.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.

9 REFERENCES

[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.

[11] E. Bresson, J. Stern, and M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In M. Yung, editor, CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, pages 465–480. Springer, 2002.

[12] J. Camenisch. Efficient and generalized group signatures. In EUROCRYPT 97, volume 1233 of Lecture Notes in Computer Science, pages 465–479. Springer, 1997.

[13] N. Chandran, J. Groth, and A. Sahai. Ring signatures of sublinear size without random oracles. In ICALP 2007, volume 4596 of Lecture Notes in Computer Science, pages 423–434. Springer, 2007.

[14] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana. Social cloud computing: A vision for socially motivated resource sharing. IEEE T. Services Computing, 5(4):551–563, 2012.

[15] D. Chaum and E. van Heyst. Group Signatures. In EUROCRYPT 91, volume 547 of Lecture Notes in Computer Science, pages 257–265. Springer, 1991.

[16] L. Chen, C. Kudla, and K. G. Paterson. Concurr ent signatures. InEUROCRYPT, volume 3027 of Lecture Notes in Computer Science, pages 287–305. Springer, 2004.

[17] H.-Y. Chien. Highly efficient id-based ring signature from pairings. In APSCC, pages 829–834, 2008.

[18] S. S. Chow, R. W. Lui, L. C. Hui, and S. Yiu. Identity Based Ring Signature: Why, How and What Next. In D. Chadwick and G. Zhao, editors, EuroPKI, volume 3545 of

Lecture Notes in Computer Science, pages 144–161. Springer, 2005.

[19] S. S. M. Chow, V. K.-W. Wei, J. K. Liu, and T. H. Yuen. Ring signatures without random oracles. In ASIACCS, pages 297–302. ACM, 2006.

[20] S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui. Efficient identity based ring signature. In ACNS 2005, volume 3531 of Lecture Notes in Computer Science, pages 499–512. Springer, 2005.

AUTHOR'S PROFILE:

SUDINI PRIYANKA

PG Scholar , Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206.

V RAMA RAO

Assistant Professor, Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206