ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2278-2566
Vol.01, Issue.04
August -2017
Pages: 400-405

COST EFFECTIVE AUTHENTIC AND ANONYMOUS DATA SHARING WITH FORWARD SECURITY

1. G.LAKSHMI DURGA, 2. J.VENKATA KRISHNA
1. PG Scholar, Dept of CSE, SREE VAHINI INSTITUTE OF SCIENCE & TECHNOLOGY, TIRUVURU
2. Associate. Professor, HOD, Dept of CSE, SREE VAHINI INSTITUTE OF SCIENCE & TECHNOLOGY, TIRUVURU

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 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.

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). 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:

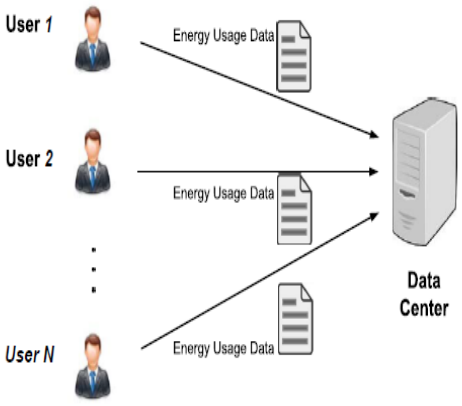

Fig. 1. Energy Usage Data Sharing in Smart Grid

Figure 1.1: Data Sharing In Smart Grid

Copyright @ 2017 ijearst. All rights reserved.

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; an

Efficiency: The number of users in a data sharing system could be HUGE (imagine a smart rid 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. 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(service is provided at an acceptable level even under network attacks) and access control (only eligible users can have the access to the data). But the study of those issues is out of the scope of this paper.

PROPOSED SYSTEM:

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 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.

ADVANTAGES OF PROPOSED SYSTEM:

• The proposed system proposes a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

• Enhancing the security of ID-based ring signature by providing forward security.

IMPLEMENTATION

MODULES:

Modules of the project

After careful analysis the system has been identified to have the following modules:

1. Authentication.
2. Data sharing.
3. Cloud computing.
4. Identity-based Ring Signature
5. Forward security,.
6. Smart grid.

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. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

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. The motto of The Royal Society is 'Nullius in verba', translated "Take no man's word for it."[1] 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.

A number of funding agencies and science journals require authors of peer-reviewed papers to share any supplemental information (raw data, statistical methods or source code) necessary to understand, develop or reproduce published research. A great

Copyright @ 2017 ijearst. All rights reserved.

deal of scientific research is not subject to data sharing requirements, and many of these policies have liberal exceptions. In the absence of any binding requirement, data sharing is at the discretion of the scientists themselves. In addition, in certain situations agencies and institutions prohibit or severely limit data sharing to protect proprietary interests, national security, and subject/patient/victim confidentiality. Data sharing may also be restricted to protect institutions and scientists from use of data for political purposes.

Data and methods may be requested from an author years after publication. In order to encourage data sharing and prevent the loss or corruption of data, a number of funding agencies and journals established policies on data archiving.

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.

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 veryuseful in many other practical application ns, especially tothose 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 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.

67

[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.

Copyright @ 2017 ijearst. All rights reserved.

[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

Copyright @ 2017 ijearst. All rights reserved.