International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 07 | Oct-2015 www.irjet.net p-ISSN: 2395-0072

Data Sharing in Cloud Using Identity Based Ring Signature

[1] Shirsath Priyanka N.,BECOMP,KVNNIEER,Maharashtra,India
[2]Rawal Sonali V.,BECOMP,KVNNIEER,Maharashtra,India
[3]Sirsat Kanchan R.,BECOMP,KVNNIEER,Maharashtra,India
[4]Tarle Gayatri P.,BECOMP,KVNNIEER,Maharashtra,India

Abstract- *Data sharing is not easier with the use of cloud computing, and an accurate analysis on the shared data provides more benefits to both the society and individuals. Data sharing with a large number of participants must take into account many issues, that is efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to build an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate the data which can be stored into the cloud or analysis purpose. Yet the most cost consuming certificate verification for public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which reduces the process of certificate verification, can be used instead. In this paper, we further improve the security of ID-based ring signature by providing forward security: If a secret key of any user has been leaked, all previous generated digital signatures that include this user still remain valid. This property is basically important to any big data sharing system, as it is impossible to ask all data owners to re authenticate their information even if a secretkey of one single user has been leaked. We provide a concrete and efficient instantiation to , prove its security and provide practicality of an implementation.*

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

1 INTRODUCTION

Ring signature for data sharing in the cloud provide secure data sharing using forward secure identity based within the group is performed in secure manner. It also provide the authenticity and anonymity of the end users. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system for end user. It allows a data owner to secretly authenticate his data which can be put into the cloud for storage. The proposed system avoids costly certificate keys for verification in the traditional public key infrastructure setting becomes a bottleneck for this solution to be scalable. Identity-based ring signature which removes the process of certificate verification can be used focused for future use. The security of ID-based ring signature by providing forward security. If a secret key of any user has been leaked, all previous generated signatures that include this user still remain valid. The 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 reveal. Accountability and privacy issues regarding cloud are becoming significant problems for cloud services. There is a lot of advancement takes place in the system with respect to the internet as a major concern in its implementation in a well effective manner respectively and also provide the system in multi-cloud environment. Many of the users are getting attracted to this technology due to the services involved in it followed by the reduced computation cost and also the reliable data transmission takes place in the system in a well effective manner respectively. The wide use of CLOUD" has brought great convenience for data sharing and collection. From the collected data a report is created, and user can compare their energy consumption with others.

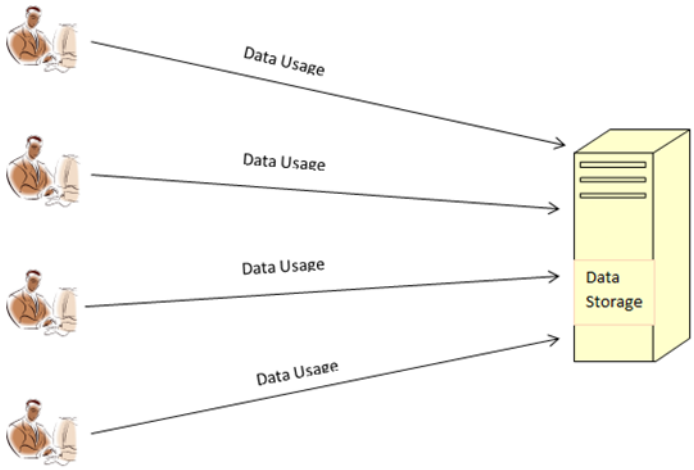

Fig. 1: Data Sharing For Energy Usage

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 accurate and detailed data/information from the levels of the electric grid is critical to efficient for energy usage. Due to its openness, data sharing is always deployed in a unfriendly environment and vulnerable to a number of security threats. In this paper enhance the security of ID-based ring signature by providing forward security. If a secret key of any user has been leaked, all previous generated signatures that include this user still remain valid. 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 statistically usage of energy data would be misleading. While this issue can be solved using well known cryptographic tools for e.g., message authentication code or digital signatures, one may encounter additional difficulties when other issues like anonymity and efficiency are taken into account.

• **Anonymity:** Energy usage data contains large information of consumers, from which one can extract the any number of persons in the home, the types of electric tools used in a specific time period, etc. Thus, it is judicial or critical to protect the anonymity of consumers in such type of applications, and any failures to do so may lead to unwillingly to share data of consumers with others.

• **Efficiency:** The number of users in a data sharing system could be LARGE, imagine a smart grid with a country size , and a practical system must reduce the computation and communication cost.

2 RELATED WORK

A robust proactive threshold signature scheme, a multisignature scheme and a blind signature scheme which work in any Gap Difie-Hellman (GDH) group (where the Computational Difie-Hellman problem is hard but the Decisional Difie-Hellman problem is easy). Constructions are simpler, more efficient and have more useful properties than similar existing constructions. Alexandra Boldyreva.[1]A ring signature scheme can be viewed as a group signature scheme with no anonymity revocation and with simple group setup. A *linkable* ring signature (LRS) scheme additionally allows anyone to determine if two ring signatures have been signed by the same group member.[2] A novel construction of ID-based ring signature which only needs two pairing computations for any group size. The proposed scheme is proven to be existential unforgeable against adaptive chosen message-and-identity attack under the random oracle model, using the forking lemma for generic ring signature schemes. We also consider its extension to support the general access structure. Sherman S.M. Chow, S.M. Yiu, and Lucas C.K. Hui[3].

Suggest solutions to the key exposure problem in ring signature. In particular, the first forward secure ring signature scheme and the first key-insulated ring signature schemes. Both constructions allow. That is, event secret keys are compromised, the validity of all forward secure ring signatures generated in the past is still preserved. In the other way, the compromise of up to all secret keys does not allow any adversary to generate a valid key-insulated ring signature for the remaining time periods. All our proposed schemes are proven secure in the random oracle model.[4] This work introduces a new provably secure group signature and a companion identity escrow scheme that are significantly more efficient than the state of the art. In its interactive, identity escrow form, our scheme is proven secure and coalition-resistant under the strong RSA and the decisional Difie-Hellman assumptions. The security of the no interactive variant, i.e., the group signature scheme, relies additionally on the Fiat-Shamir heuristic (also known as the random oracle model).[5]
This paper provides theoretical foundations for the group signature primitive. We introduce strong, formal definitions for the core requirements of anonymity and traceability. We then show that these imply the large set of sometimes ambiguous existing informal requirements in the literature, thereby unifying and simplifying the requirements for this primitive. Finally we prove the existence of a construct meeting our definitions based only on the assumption that trapdoor permutations exist. Daniele Micciancio*y* [6].

Improve the Bellary-Miner (Crypto '99) construction of signature schemes with forwardsecurity in the random oracle model. Our scheme has significantly shorter keys and is, therefore,more practical. By using a direct proof technique not used for forward-secure schemes before,we are able to provide better security bounds for the original construction as well as for

ourscheme. Beglare and Miner also presented a method for constructing such schemes without the useof the random oracle. We conclude by proposing an improvement to their method and an additional, new method for accomplishing this.[7] A new ID-based ring signature scheme and a proxy ring signature scheme. Both the schemes are more efficient than existing one. These schemes also take care of the inconsistencies in above two schemes. A ring signature is a simplified group signature without any manager. It protects the anonymity of a signer. The first scheme proposed by Rivest et al. was based on RSA cryptosystem and certificate based public key setting. Amit K Awasthi1 and Sunder Lal [8]

3 SYSTEM FLOW

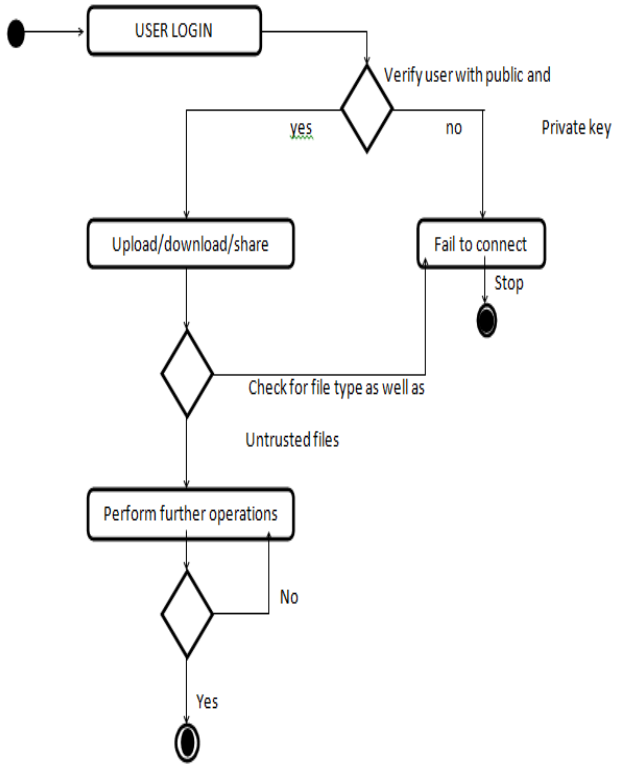

Fig. 2: System Flow Design

4 APPLICATIONS

Whistle Blowing:

You are a whistle blower if you are a worker and you report certain types of wrong doing. This will usually be something you've seen at work - though not always. The wrongdoing you disclose must be in the public interest. This means it must affect others, e.g. the general public. As a whistle blower you're protected by law - you should be treated unfairly or lose your job because you blow the whistle.

You can raise your concern at any time about an incident that happened in the past, is happening now or you believing will happen in the near future. 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 Bobs identity. The disclosure by a person, usually an employee in a government agency or private enterprise, to the public or to those in authority, of mismanagement, corruption, illegality, or some other wrongdoing. The public value of whistle-blowing has been increasingly recognized. For example, federal and state statutes and regulations have been enacted to protect whistleblowers from various forms of retaliation.

E-Contract Signing:

Electronic signature schemes have become big business. In fact, the e-signing sector is on track to grow north of 5 billion by the end of the decade, according to DocuSign CMO Dustin Grosse. E-signing tools represent a high-tech and much-needed response to the vast in efficiencies of dealing with physical signatures. 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. 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.

5 CONCLUSION

As the practical needs in data sharing, this paper proposed a new notion called Forward Secure ID-Based Ring Signature. This allows an ID-based ring signature scheme with the feature of forward security. It is the first in the literature to have this type of feature for ring signature in ID-based setting. Our scheme provides unconditional anonymity and can be proven forward-secure unforgettable in the random oracle model, assuming RSA problem is hard. This proposed scheme is very efficient and it 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, ecommerce 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] 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 inComputer Science, pages 31–46. Springer, 2003.

[2] Patrick P. Tsang and Victor K. Wei Short Linkable Ring Signatures for E-voting, E-cash and Attestation. Department of Information EngineeringThe Chinese University of Hong KongShatin, Hong Kong *f*pktsang3,kwwei*g*@ie.cuhk.edu.hk

[3] 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.

[4] J. K. Liu and D. S. Wong. Solutions to key exposure problem in ring signature. I. J. Network Security, 6(2):170–180, 2008.

[5] 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.

[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 ComputerScience, pages 431–448. Springer-Verlag, 1999.

[8] A. K. Awasthi and S. Lal. Id-based ring signature and proxy ring signature schemes from bilinear pairings. CoRR, abs/cs/0504097, 2005.

BIOGRAPHIES

Shirsath Priyanka Nandkumar
Department Of Computer Engineering,
KVNNIEER, Pune University,
Maharashtra.

Rawal Sonali Vijaysing
Department Of Computer Engineering,
KVNNIEER, Pune University,
Maharashtra.

Sirsat Kanchan Ramdas
Department Of Computer Engineering,
KVNNIEER, Pune University,
Maharashtra.

TarleGayatri Prakash
Department Of Computer Engineering,
KVNNIEER, Pune University,
Maharashtra.