IJRSET MARCH 2017 Volume 4, Issue 3 Pages: 20-26

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

FILE SECURITY USING RING SIGNATURE BASED ROLE ACCESS CONTROL MECHANISM

[1] PL. Rajarajeswari, [2] R. Ashwin, [3] C. Vasanthkumar, [4] R.B. Manikannden
[1] ME- Assistant Professor, [2, 3, 4] BE,
[1, 2, 3, 4] Sri Krishna College of Technology, Coimbatore.

ABSTRACT: The key feature of cloud computing is one can access information any place, anywhere, at any time. So basically cloud computing is subscription based service where one can obtain network storage space and computer resources for data storage as well as data sharing. Due to high fame of cloud for data storage and sharing, large number of participants gets attracted to it but it leads to issue related to efficiency, Data integrity, privacy and authentication. To overcome these issues, concept of ring signature has been introduced for data sharing amongst large number of users. Ring signatures are used to provide user's anonymity and signer's privacy. 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. Session based ID with ring mechanism helps to implement session based key and access files within a session. Use of ID-based ring signature, removes the need of certificate verification which was done using public key infrastructure, hence reduce cost as well as introduction of forward security, further strengthen this system more. Use of weil pairing, keeps even shorter keys secure and it also requires less processing power. So the motivation of this paper is to propose a secure data reading and sharing scheme using above mentioned scheme.

1. INTRODUCTION

Over the past few years, cloud computing has rapidly emerged as a successful paradigm for providing IT infrastructure, resources and services on a pay-per-use basis. The wider adoption of Cloud and virtualization technologies has led to the establishment of large scale data centers that provide cloud services. This evolution induces a tremendous rise of electricity consumption, escalating data center ownership costs and increasing carbon footprints. For these reasons, energy efficiency is becoming increasingly important for data centers and Cloud. The fact that electricity consumption is set to rise 76% from 2007 to 2030 with data centers contributing an important portion of this increase emphasizes the importance of reducing energy consumption in Clouds. challenges. Provided solutions should scale in multiple dimensions and Cloud providers must also deal with the users' requirements which are being more and more complex. Requested services are more sophisticated and complete since users need to deploy their own applications with the topology they choose and with having the control on both

infrastructure and programs. This means combining the flexibility of IaaS and the ease of use of PaaS within a single environment. As a result, the classic three layer model is changing and the convergence of IaaS and PaaS is considered as natural evolutionary step in cloud computing. Cloud resource allocation solutions should be flexible enough to adapt to the evolving Cloud landscape and to deal with users requirements. Another important dimension we consider is the type of the virtualization. In addition to traditional VM based technology, Cloud providers are also adopting new container-based virtualization technologies like LXC and Docker that enable the deployment of applications into containers. Hence, this resource variety aspect should be taken into account when modeling the problem of resource allocation to scale with the Cloud evolution and with new users requirements. One last important dimension at which we are interested in this work is the resource provisioning plan. Cloud providers could offer two types of resource provisioning: on-demand and advance or long-term reservation. Advance reservation concept has many advantages especially for the co-allocation for resources. It provides simple means for resource planning and reservation in the future and offers an increased expectation that resources can be allocated when demanded. Although advance reservation of resources in cloud is very advantageous, the focus has been mostly on the on-demand plan. Ring signatures are very useful tools for many privacy-preserving applications. However, they are not adequate in settings where some degree of privacy for users must be balanced against limited access. For example, a service provider might have the list of public keys that correspond to all users that have purchased a single access to some confidential service for that day (requiring anonymous authentication). For this kind of application, a number of restricted-use ring signatures are proposed. Notable examples include linkable ring signatures and traceable ring signatures. Linkable ring signature asks that if a user signs any two messages (same or different) with respect to the same ring, then an efficient public procedure can verify that the signer was the same (although the user's identity is not revealed). Traceable ring signature is a ring signature scheme where each message is signed not only with respect to a list of ring members, but also with respect to an issue (e.g., identifying label of a specific election or survey). If a user signs any two different messages with respect to the same list of ring members and the same issue label, then the user's identity is revealed by an efficient public procedure.

2. RELATED WORKS

Large networks like the internet, the centralistic approach of IBE becomes problematic. Of course, one could adapt the existing CA system so that parameters for multiple PKGs are automatically deployed with common software packages. However, a major drawback is the implicit key escrow which does not exist with the current classical framework. Although some bureaucrats would surely like this idea, history has shown that systems designed to ensure privacy with secret backdoors are not accepted as they take the actual goal ad absurdum. To enable wide-spread use, these problems have to be overcome first. Another completely different topic is that the mathematics behind IBE (considering for instance the presented scheme) are in many cases far more complicated than those for RSA, ElGamal or DSA. This makes implementation difficult, especially since less experience and resources are available on the rather young field of pairing based crypto. Divertible Protocols and Atomic Proxy Cryptography [1] A basic goal of public-key encryption is to allow only the key or keys selected at the time of encryption to decrypt the ciphertext. To change the ciphertext to a different key requires re-encryption of the message with the new key, which implies access to the original cleartext and to a reliable copy of the new encryption

key. A Closer Look at PKI: Security and Efficiency [2] **S**ecurity of the basic primitives in this more complex setting. We also provide constructions for encryption and signature schemes that provably satisfy our strong security definitions and are more efficient than the corresponding traditional constructions that assume a digital certificate issued by the CA must be verified whenever a public key is used. Identity-Based Proxy Re-Encryption [3] semi-trusted keyserver re-encrypts these encapsulated symmetric keys from the master key to the keys of individual users who can then decrypt. The key server provides access control for the encrypted material, but does not itself possess the ability to decrypt files. This application use key to specify access control policies directly within the identity strings of the users. Proxy Re-encryption Systems for Identity-based Encryption [4] Identity-Based Encryption (for short, IBE) has been one of the most active research area. In the IBE system, a sender Catherine encrypts a message to an IBE receiver Alice by using Alice's identity as a public key. A Type-and-Identity-based Proxy Re-Encryption Scheme and its Application in Healthcare [5] we propose a type-and-identity-based proxy re-encryption scheme based on the Boneh-Franklin IBE scheme to enable the delegator to implement different access control policies for his cipher texts against his delegates. Identity-Based Conditional Proxy Re-Encryption [6] to overcome the limitation of existing IBPRE, we introduce the notion of Identity-based conditional proxy re-encryption (IBCPRE), whereby only cipher text satisfying one condition set by delegator can be transformed by the proxy and then can be decrypted by delegate. Conditional Proxy Re-Encryption Secure against Chosen-Ciphertext Attack [7] The proxy can then convert any cipher- text under Alice's public key into ciphertext under Bob's public key. The requirement is that the semantic security of encryptions for Alice is preserved throughout the conversion, such that the proxy gains no information about the involved plaintext messages.

3. PROPOSED SYSTEM

The proposed system is a signature based role access control mechanism, also known as role-oriented ring signature. In this scheme, only the person who belongs to the designated role can verify the validity of the ring signature. In role-oriented signature, nobody besides the designated role can verify the signature. Obviously, in a PKI authentication frame, each person should have his own key pair. So the core issue of role-oriented signature is how to design a scheme in which each role member is allowed to verify the signature independently. As we have mentioned above, a ring signature with limited verification range is necessary in some instances. A signer can perform following steps to produce a role-oriented ring signature. Session based authentication and file sharing added a more advantages in this system. The receiver identity is mainly considered while receiving the file and also during re-encryption.

- The identity signature and role are considered to identify the receivers
- High secure to the system by generating unique signature for each users.
- Three factors combination will give the high secure for the users data transmission.

3.1 User Interface Design

The main idea of this module is to design the user interface for users in the project. The login page is to design for data owner and data user. After the data owner logins into the system, the page displayed which allows the data owner to achieve the encrypted file upload to the system. When the user logins to the system, the system allows the user to input the decryption key and attributes for retrieval of specified file. Before accessing the file from system, the user must register into the system. And based on their role, the user can able to retrieve the data.

3.2 File Encryption

Each file which is to be uploaded is encrypted with encryption key. Once file is encrypted, next step is to upload it to the storage system along with data decryption key. Owner specifies the set of attributes for access structure, it then encrypts the file. Finally, owner uploads encrypted file and encryption key and set of attributes to the storage system.

3.3 Key Generation and Distribution

While data owner uploading the encrypted file, they also upload set of attributes. The data owner gives the attributes of the receiver while sending the file to the receiver; the file gets encrypted as per the given attributes. Thus the attributes for specified file is to be distributed and decryption key for decrypting the file are to be distributed to the data users. Sign based role access control mechanism also known as role-oriented ring signature is used in this module.

3.4 Multiple Data Sharing

User requests the file by providing details and in response system replies with encrypted file. Before that the system will check the role and signature of the users whether the receiver have the same role as the sender mentioned. It will avoid the unauthorized users or hackers. The receiver receives the encrypted file, and he has correct role and signature, if it's correct, the original file gets decrypted for the receiver. This allows them to access information without authorization and thus poses a risk to information privacy.

4. METHODOLOGY

Prior work on ring signature/identification schemes provides definitions of security that are either rather informal or seem (to us) unnaturally weak, in that they do not address what seem to be valid security concerns. One example is the failure to consider the possibility of adversarial-chosen public keys. Specifically, both the anonymity and unforgeability definitions in most prior work assume that honest users always sign with respect to rings consisting entirely of honestly-generated public keys; no security is provided if users sign with respect to a ring containing even one adversarial-generated public key. Clearly, however, a scheme which is not secure in the latter case is of limited use; this is especially true since rings are constructed in an ad-hoc fashion using keys of (possibly unknown) users which are not validated as being correctly constructed by any central authority. We formalize security against such attacks (as well as others), and show separation results proving that our definitions are strictly stronger than those considered in previous work. In addition to the new, strong definitions we present, the hierarchy of definitions we give is useful for characterizing the security of ring signature constructions.

We present three ring signature schemes which are provably secure in the standard model. We stress that these are the first such constructions, as all previous constructions of which we are aware rely on random oracles/ideal ciphers. It is worth remarking that ring identification schemes are somewhat easier to construct (using, e.g., techniques from ring signatures can then easily be derived from such schemes using the Fiat-Shamir methodology in the random oracle model. This approach, however, is no longer viable (at least, based on our current understanding) when working in the standard model.

Definition

We begin by presenting the functional definition of a ring signature scheme. We refer to an ordered list $R = (P K_1, \ldots, P K_n)$ of public keys as a ring, and let $R[i] = P K_i$. We will also freely use set notation, and say, e.g., that $P K \in R$ if there exists an index i such that $R[i] = P K$. We will always assume, without loss of

generality, that the keys in a ring are ordered lexicographically.

Definition 1 [Ring signature] A ring signature scheme is a triple of ppt algorithms (Gen, Sign, Vrfy) that, respectively, generate keys for a user, sign a message, and verify the signature of a message. Formally:

- Gen(1^k), where k is a security parameter, outputs a public key P K and secret key SK .
- $\text{Sign}_{s,S\ K}$ (M, R) outputs a signature σ on the message M with respect to the ring R = (P K_1 , . . . , P K_n).
- We assume the following: (1) (R[s], SK) is a valid key-pair output by Gen; (2) |R| ≥ 2 (since a ring signature scheme is not intended[2] to serve as a standard signature scheme); and each public key in the ring is distinct.
- Vrfy_R (M, σ) verifies a purported signature σ on a message M with respect to the ring of public keys R.

We require the following completeness condition to hold: for any integer k, any $\{(PK_i, SK_i)\}_{i=1}^{n}$ output by Gen(1^k), any s ∈ [n], and any M , we have Vrfy_R (M, $\text{Sign}_{s,S\ K}$ (M, R)) = 1 where R =(P K_1 , . . . , P K_n). A c-user ring signature scheme is a variant of the above that only supports rings of fixed size c (i.e., the Sign and Vrfy algorithms only take as input rings R for which |R| = c, and correctness is only required to hold for such rings).

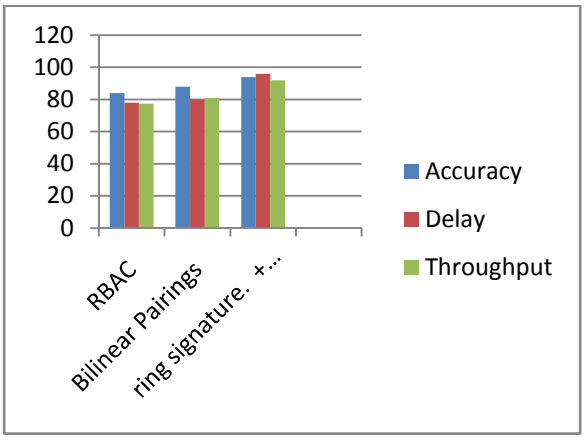
To improve readability, we will generally omit the input "s" to the signing algorithm (and simply write σ ← Sign_{SK} (M, R)), with the understanding that the signer can determine an index s for which SK is the secret key corresponding to public key R[s]. Strictly speaking, there may not be a unique such s when R contains incorrectly-generated keys; in real-world usage of a ring signature scheme, though, a signer will certainly be able to identify their public key. A ring signature scheme is used as follows: At various times, some collection of users runs the key generation algorithm Gen to generate public and secret keys. We stress that no coordination among these users is assumed or required. When a user with secret key SK wishes to generate an anonymous signature on a message M , he chooses a ring R of public keys which includes his own, computes σ ← Sign_{SK} (M, R) and outputs (σ, R). (In such a case, we will refer to the holder of SK as the signer of the message and to the holders of the other public keys in R as the non-signers.) Anyone can now verify that this signature was generated by someone holding a key in R by running Vrfy_R (M, σ). We remark that although our functional definition of a ring signature scheme requires users to generate keys specifically for that purpose (in contrast to the requirements of our first construction can be easily modified to work with any ring of users as long as they each have a public key for both encryption and signing.

5. EXPERIMENT RESULT AND DISCUSSION

An experimental role-based cryptosystem was implemented to test the feasibility of our schemes. This system was developed with a standard Java language in QT environment, which supports cross-platform deployment. This system consists of three modules: RBC module, access control module and application module. In RBC module, we adopted GNU multiple precision arithmetic library (GMP) to handle integers of arbitrary precision. Then, a finite fields arithmetic library was constructed to realize the run-time environment of elliptic curve and pairing-based cryptosystems. In addition, a cryptographic access control library was developed based on the control.

Compared to existing algorithms our performance is increased. The below tables

represent the accurate values of current process and existing values.



The individual accuracy rates obtained from different feature selection methods on the classifier. Different feature selection metrics are applied on the classifier.

CONCLUSION

The ring signature technique that uses an ad-hoc group of signer identities is a widely used method for generating this type of privacy preserving digital signatures. The identity based cryptographic techniques do not require certificates. The construction of ring signatures using identity-based cryptography allow for privacy preserving digital signatures to be created in application when certificates are not readily available or desirable such as in vehicle area networks. We propose a new designated verifier identity based ring signature scheme that is secure against full key exposure attacks even for a small group size. This is a general purpose primitive that can be used in many application domains such as ubiquitous computing where signer ambiguity is required in small groups.

REFERENCE

[1] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Crytographic Techn.: Adv. Cryptol., 1998, pp. 127–144.

[2] A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi, “A closer look at PKI: Security and efficiency,” in Proc. 10th Int. Conf. Practice Theory Public-Key Cryptography, 2007, pp. 458–475.

[3] M. Green and G. Ateniese, “Identity-based proxy re-encryption,” in Proc. 5th Int. Conf. Appl. Cryptography Netw. Security, 2007, pp. 288–306.

[4] T. Matsuo, “Proxy re-encryption systems for identity-based encryption,” in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 247–267.

[5] C.-K. Chu and W.-G. Tzeng, “Identity-based proxy re-encryption without random oracles,” in Proc. 10th Int. Conf. Inf. Security, 2007, pp. 189–202.

[6] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, “A type-and-identity- based proxy re-encryption scheme and its application in healthcare,” in Proc. 5th VLDB Conf. Secure Data Manage., 2008, pp. 185–198.

[7] J. Shao, G. Wei, Y. Ling, and M. Xie, “Identity-based conditional proxy re-encryption,” in Proc. IEEE Int. Conf. Commun., 2011, pp. 1–5.

[8] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang, “A CCA-secure identity-based conditional proxy re-encryption without random oracles,” in Proc. 15th Int. Conf. Inf. Security Cryptol., 2012, pp. 231–146.

[9] C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, “Conditional proxy broadcast re-encryption,” in Proc. 14th Australasian Conf. Inf. Security Privacy, 2009, pp. 327–342.

[10] Q. Tang, “Type-based proxy re-encryption and its construction,” in Proc. 9th Int. Conf. Cryptol. India: Progress Cryptol., 2008, pp. 130–144.

[11] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, “Conditional proxy re-encryption secure against chosen-ciphertext attack,” in Proc. 4th Int. Symp. Inf., Comput. Commun.Security, 2009, pp. 322–332.

[12] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, “Efficient conditional proxy re-encryption with chosen-ciphertext security,”

in Proc. 12th Int. Conf. Inf. Security, 2009, pp. 151–166.
[13] L. Fang, W. Susilo, and J. Wang, “Anonymous conditional proxy re-encryption without random oracle,” in Proc. 3rd Int. Conf. Provable Security, 2009, pp. 47–60.
[14] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang, “A conditional proxy broadcast re-encryption scheme supporting timedrelease,” in Proc. 9th Int. Conf. Inf. Security Practice Experience, 2013, pp. 132–146.
[15] P. R. Zimmermann, PGP Source Code and Internals. Cambridge, MA, USA: MIT Press, 1995.
[16] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in Proc. 21st Annu. Int. Cryptol.: Adv. Cryptol., 2001, pp. 213–239.
[17] Radicati Group. (2014). Cloud business email market, 2014-2018 [Online]. Available: http://www.radicati.com/wp/wp-content/\uploads/2014/10/Cloud-Business-Email-Market-2014-2018-Executive-Summary.pdf
[18] Proofpoint Group. (2012). Cloud-based archiving vs. on-premises legacy archiving [Online]. Available: http://video.proofpoint.com/id/cloud-based-archiving-vs.-on-premises-legacy-archiving-TCO-white-paper