International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 10|| October 2017 || PP. 17-22

An Enhanced Framework for Uniqueness Based Protected and Supple Data distribution in Cloud Based Smart Network

Venkateswarlu Sunkari
Assistant Professor, Addis Ababa Institute of Technology, Addis Ababa, Ethiopia.
v.sunkari@aait.edu.et

Abstract: *Data distribution and analysis are important utilities in real world applications. The possibility of making proficient resolutions based on analyzed data. On other hand, so many issues include data privacy and authentication, Integrity, efficiency and security. There is a mounting need of flexibility and security for sharing data among users of grid in cloud environment. It is continuous process to build mechanisms to overcome these issues. Yet, it is immense challenge to have a solution for security and flexibility in cloud computing environment for data sharing. Uniqueness -based ring signature provides solution to the problem for existing system which was proposed by Huang et al. This system was able to build a system with authentication and anonymity thus preserving privacy of data owners. Also eliminates the usage of Public Key Infrastructure that needs certificate verification which is costly and reduces scalability of the systems. They also provided forward security to make the system scalable. However, this system was based on standard RSA assumption of random oracle model that can be improved further. In this paper a system has been proposed which is aimed at building an Enhanced Uniqueness-based protected and supple data distribution in cloud based Network. Moreover, proposed system strives to build a robust enhanced Uniqueness-based protected data distribution system that improves intuitiveness in the secure communications.*

Keywords: *Cloud computing, Data distribution, Forward Security, privacy, Authentication.*

Date of Submission: 05-09-2017 Date of acceptance: 14-10-2017

I. Introduction

Cloud computing has emerged to provide plenty of benefits to individuals and organizations. With cloud data distribution became easier. Individuals can have convenience of storage in cloud besides sharing it with intended users. Smart grid [20] is one among the example that can exploit cloud storage services for sharing data. Users of smart network can store and retrieve their energy usage data besides helping others to view it by sharing. When such data is available, the energy utilization behavior of various users can be mined and used for building good strategies. This ability to storage, manage, analyze and make well informed decisions on stored data is critical for users of smart network. However, the data is outsourced to cloud where data will be stored in servers are treated by users as unbelievable. This is the main problem with data outsourcing and distributing with data. In this context, naturally, there are security concerns. To address this problem it is necessary to have a flexible mechanism that can help in protecting data and sharing it with required security. With respect to energy usage data of smart network stored in cloud, it is important to have data integrity. When misleading data is stored by adversaries which causes issues to genuine users. Therefore it is necessary to avoid such issues while distributing data to others. The data owner needs to form a group and share data across the group members. In the process authentication is very important and then authorization and anonymity if required. Anonymity is needed as it is not important to know whose data it is. Energy sage data of a smart network contains information such as number of people living in a home, the electronic utilities, and specific time period. At the same time it is important to have anonymity of consumers while using the applications. When anonymity is not provided to users, it causes potential security risk. When number of users share data present in cloud, the computational complexity is high. This needs to be reduced as it contradicts the goal of a smart network in the real world. When the smart grid spans entire country, it is inevitable to have effective data sharing mechanisms that provides security and convenience. Without time and Geographical restrictions, one can gain access to cloud. The computation cost and communication cost are to be monitored and they are to be reduced with continuous optimization. Framework has been proposed and implemented that takes care of Identity Based secure data sharing mechanism. This paper includes design and implementation of a framework that helps in facilitating the data through secure data sharing. Proposed system is flexible and ensures that the cloud data can be shared while preserving security issues. The remainder of the paper is structured as follows. Literature survey is described in the Section II, and Section III presents the proposed system in detail. Section IV presents comparison results, while paper will be concluded with section V.

II. Related Works

Identity-based cryptosystem which is proposed by Shamir [1], excludes the use for verifying the foundation of public key certificates which is both time and cost exhausting. Public key of each and every user In an ID-based cryptosystem, the public key of each and every user can be easily computed from their publicly known identity information (e.g., an email address, or residential address, etc.). A private key generator (PKG) then generates private keys for each and every user present in the group from their master secret. Which will avoids the need of certificates (which is essential in traditional public-key infrastructure) and associates a corresponding public key (user identity) to each and user within the system. ID-based signature is different from traditional Ring –based signature will eliminates the certificate verification. The elimination of this certificate validation makes the whole verification process more efficient, Which will lead to a eloquent save in both communication and computation when a large number of users will be involved (say, which is energy usage data in smart-grid). Ring signature is a process of group-oriented process with privacy protection. A user in the group can send message anonymously on his own choice, while the members of that group will be totally unaware of being constrained in the group. Any verifier in that group can be convinced that a message is from any one of the group member (also called as Rings), but the actual identity of the sender is hidden. Ring signatures can be used for whistle blowing [2], for ad hoc groups [3] and many other applications which do not want to make complicated group formation stage but require signer anonymity. There have been many different schemes proposed (e.g., [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15]) since the first appearance of ring signature in 1994 [16] and the formal introduction in 2001 [2]. The first ID-based signature scheme was proposed in 2002 [17] which has be evince security in random oracle model. Two constructions present in the standard model were proposed in [18]. Their first construction was discovered as the flaw [19], while the second construction is only evince secure in a weaker model, namely, selective-ID model.

The drawback of existing system is that there is random oracle assumption that is used in the research. This assumption may work as theoretical black box without real implementation of primitives to some extent. Random oracle takes inputs and provides pre-defined responses with respect to cryptographic operations.

Random oracle is in fact a mathematical abstraction that makes the work of researchers easier. However, it has certain pre-defined functionality and acts like a black box which takes input and gives a pre-defined response. Thus random oracle assumption, sometimes, may not reflect true dynamics required in the real world system.

In this paper we used real cryptographic primitives as part of the proposed system. Unlike random oracles that act as black box and provides convenience without real implementation, our work used real cryptographic functionalities without using random oracles assumption. Thus it can reflect true dynamics of the system besides helping the researcher to understand the consequences of using and not using such security primitives.

III. Preliminaries

This section provides required prerequisites to understand the proposed system. It throws light into symmetric, asymmetric cryptography besides the Identity Based Cryptography.

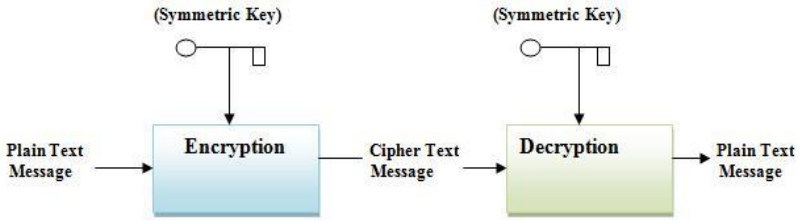

Figure 1 – Symmetric cryptography

As shown in Figure 2, Here same key will be used for both decryption and encryption. The problem with this kind of cryptography is key sharing in a secure fashion. To overcome this asymmetric cryptography came into existence.

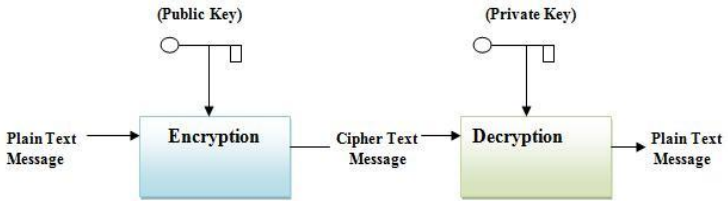

Figure 2 – Asymmetric cryptography

As shown in Figure 2, it is evident that there are two keys involved in the cryptographic process. Public key of receiver is used for encryption and the private key of the receiver is used for decryption. This can effectively avoid key sharing over network. Hence it is more secure than its symmetric counterpart.

3.1 Enhanced Uniqueness Based Cryptography

Identity is any publicly available ID of a user or organization. For instance email is an example for publicly known identity. The usage of such key in the process of encryption makes it more intuitive and user-friendly. The end user need not to have the knowledge of keys in cryptography.

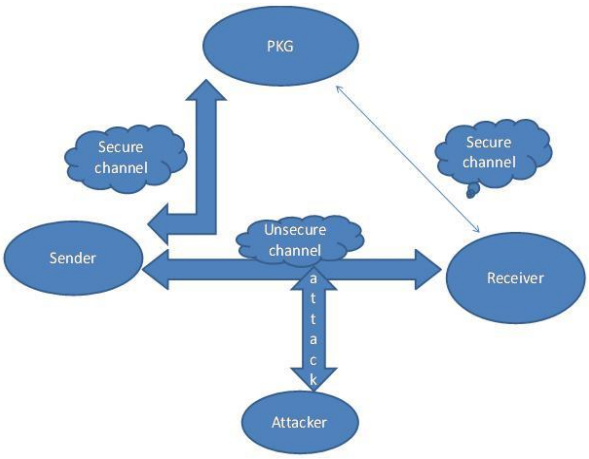

Figure 3 – Enhanced Uniqueness based cryptography.

As shown in Figure 3, EUBC does not need any certificate authority to provide keys. It simply needs a program that can generate private keys. Secure communications are possible between two parties without having issues with eavesdropper due to the asymmetric nature of the cryptographic primitives employed.

IV. Proposed Data Sharing Model

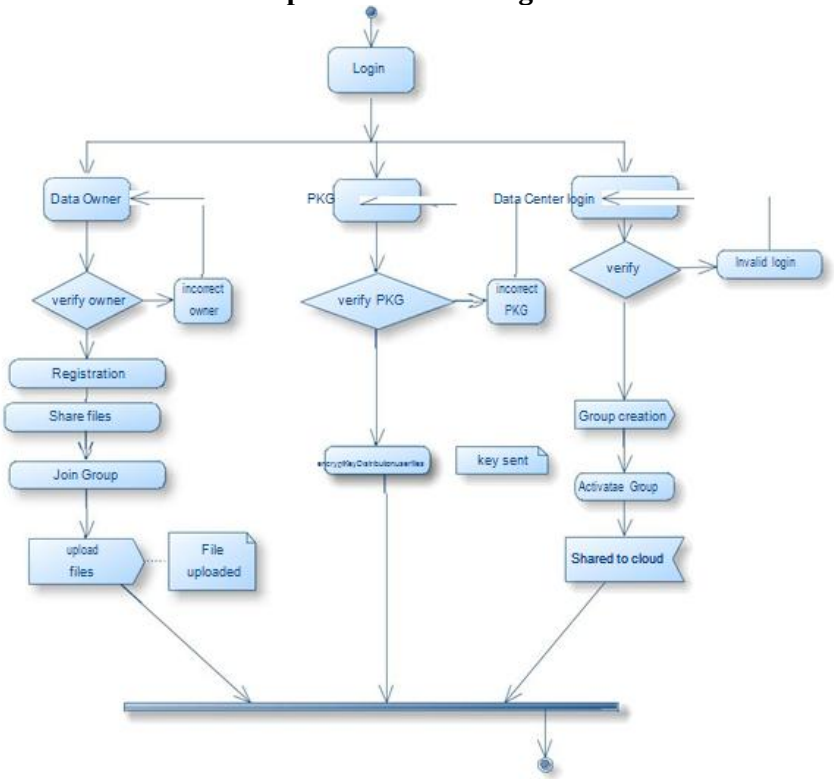

Figure 4 – Activities of users in the system

The proposed system has three important modules that work in secure sharing of data. Data centre, data owner and PKG. The PKG is responsible to generate keys and key distribution. It is aware of ID based cryptography. The data centre module facilitates users to create groups, activating groups and data sharing in secure fashion. The data owner is responsible to upload files, view shared files and join groups that have been created. Figure 4 will illustrates the interaction and activities of different parties involved in the system.

There is authentication process implemented in the proposed system. It is responsible for ensuring that only authorized participants can use the system. Data sharing is the process of allowing other users to gain access to data outsourced to cloud. Again this act is based on the real world need and the privileges bestowed to other users on data. Identity-based was first introduced by Shamir. It is used in this system to have identity based ring signature. The presence of PKG in the proposed system improves security besides avoiding the usage of certificate authorities. The EIBC is different from traditional public key cryptography.

Algorithm:

1. PKG generates public key and private key
2. Sender obtains master public key from PKG
3. Sender requests for his private key
4. PKG provides private key to sender
5. Receiver obtains master public key from PKG
6. Receiver requests for his private key
7. PKG provides private key to receiver

Once both parties are with private keys they can exchange messages

8. Sender uses public key of receiver to encrypt message and send it to receiver
9. Receiver can decrypt the message with his private key
10. Thus mutual key establishment and secure communication is completed

As shown in algorithm, it is evident that IBC is nothing it is public key cryptography which uses two separate keys are used for encryption and for decryption. This concept is exploited in this project for group of users and there is the concept of data sharing. We implemented a prototype application using Java platform. The application is web based and multiple types of users can have sessions simultaneously. There is key distribution process demonstrated.

V. Experimental Results

Experiments are made with number of users in the ring and the average time taken for various activities such as signing the usage data and the verification of ring signature with different time periods.

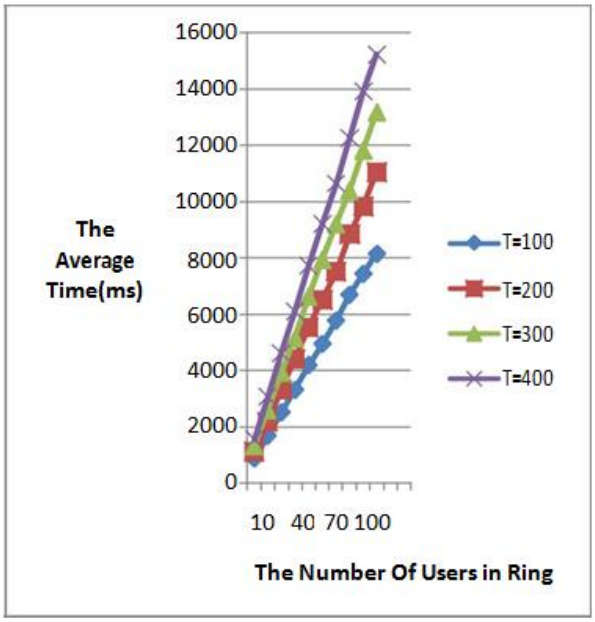

Figure 6 – Average time taken for data owner to sign usage data

As shown in Figure 6, The horizontal axis represents number of users in the ring while the vertical axis represents average time taken for data owner to sign usage data. Here The average time is directly proportional to the number of users and the time period considered.

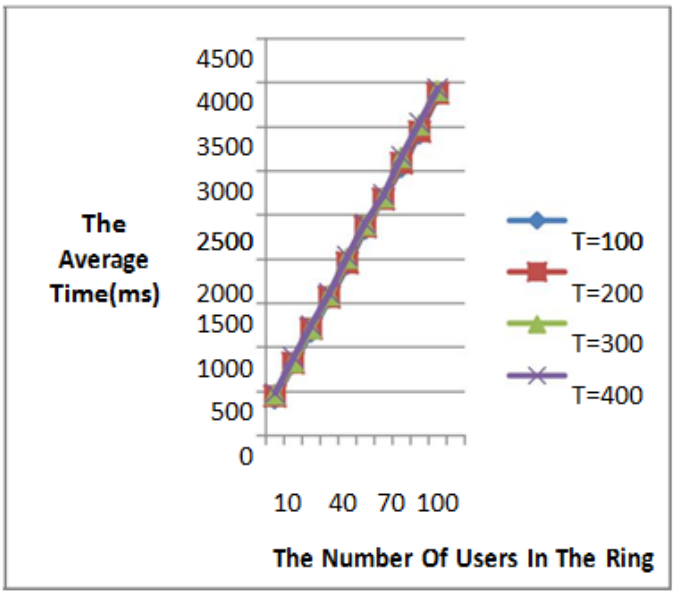

Figure 7 – Average time verification of ring signature

As shown in Figure 7, it is evident that the horizontal axis represents number of users in the ring while the vertical axis represents average time taken for verification of ring signature. Here The average time is directly proportional to the number of users and the time period .

VI. Conclusions And Future Work

In this paper that cryptographic primitives is used for securing data in the cloud. Especially we focused on the secure distribution of cloud data. We found Enhanced Uniqueness based cryptography is cost-effective and flexible due to the usage of PKG without depending on costly certificates. We used the notion of ring signature in order to have efficient group management. Groups are managed for efficient security management. We proposed an algorithm for Enhanced Uniqueness based cryptography. We built a prototype application that facilitates different users to perform their respective activities. The application demonstrates secure distribution of keys and there is authentication and authorization process in order to have efficient data distribution in cloud. Our empirical results reviled that the proposed scheme is effective and supports multiple users in ring with session management. This can be extended further using Symmetric and Asymmetric Identity based cryptography schemes.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO 84 Adv. Cryptol., 1984, vol. 196, pp. 47–53.
[2] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in Proc. 7th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol., 2001, vol. 2248, pp. 552–565.
[3] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in Proc. 22nd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2002, vol. 2442, pp. 465–480.
[4] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol., 2002, vol. 2501, pp. 415–432.
[5] N. Chandran, J. Groth, and A. Sahai, "Ring signatures of sublinear size without random oracles," in Proc. 34th Int. Colloq. Automata, Lang. Programming, 2007, vol. 4596, pp. 423–434.
[6] S. S. M. Chow, V.K.-W. Wei, J. K. Liu, and T. H. Yuen, "Ring signatures without random oracles," in Proc. ACM Symp. Inform., Comput., Commun. Security, 2006, pp. 297–302.
[7] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in Ad Hoc groups," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, vol. 3027, pp. 609–626.
[8] D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo, and D. S. Wong, "Revocable ring signature," J. Co mput. Sci. Tech., vol. 22, no. 6, pp. 785–794, 2007.
[9] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Online/offline ring signature scheme," in Proc. 11th Int. Conf. Inform. Commun. Security, 2009, vol. 5927, pp. 80–90.
[10] J. K. Liu, W. Susilo, and D. S. Wong, "Ring signature with designated linkability," in Proc. 1st Int. Conf. Security, 2006, vol. 4266, pp. 104–119.

[11] J. K. Liu, V. K. Wei, and D. S. Wong, "A separable threshold ring signature scheme," in Proc. 6th Int. Conf. Inform. Security Cryptol., 2003, vol. 2971, pp. 12–26.
[12] J. K. Liu and D. S. Wong, "On the security models of (Threshold) ring signature schemes," in Proc. 6th Int. Conf. Inform. Security Cryptol., 2004, pp. 12–26.
[13] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," IEEE Trans. Inform. Theory, vol. 57, no. 7, pp. 4833–4842, Jul. 2011.
[14] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," in Proc. 10th Int. Conf. Practice Theory Public Key Cryptography, 2007, vol. 4450, pp. 166–180.
[15] D. S. Wong, K. Fung, J. K. Liu, and V. K. Wei, "On the RS-Code construction of ring signature schemes and a threshold setting of RST," in Proc. 5th Int. Conf. Inform. Commun. Security, 2003, vol. 2836, pp. 34–46.
[16] R. Cramer, I. Damga rd, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in Proc. 14th Annu. Int. Cryptol. Conf. Adv. Cryptol., 1994, vol. 839, pp. 174–187.
[17] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security, 2002, vol. 2501, pp. 533–547.
[18] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, "ID-based ring signature scheme secure in the standard model," in Proc. 1st Int. Workshop Security Adv. Inform. Computer. Security, 2006, vol. 4266, pp. 1–16.
[19] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen. (2009). Practical short signature batch verification," in Proc. Cryptographers' Track RSA Conf. Topics Cryptol., vol. 5473, pp. 309– 324 [Online]. Available: http://eprint.iacr.org/2008/015
[20] National Institute of Standards and Technology. NIST IR 7628: Guidelines for Smart Grid Cyber Security, August 2010.

Venkateswarlu Sunkari. "An Enhanced Framework for Uniqueness Based Protected and Supple Data distribution in Cloud Based Smart Network ." International Journal of Engineering Science Invention(IJESI), vol. 6, no. 10, 2017, pp. 17–22.