ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Data Storage in Cloud using forward Security and ID-based Ring Signature

Dr. K. Praveen Kumar[1], Desalegn Abebaw[2]

Assistant Professor, Computer Science Engineering Program, Adama Science & Technology University, Ethiopia[1]

Lecturer, Computer Science Engineering Program, Adama Science & Technology University, Ethiopia[2]

ABSTRACT: Due to the advance of incipient technology data sharing has never been more facile in this world. A precise analysis on the shared data provides a group of benefits to both the society and individuals. Data sharing between two members or group of members must take into account several issues. They are efficiency, data integrity and privacy of data owner. To surmount this issue Ring signature concept is introduced. It is a promising approach to construct a secret and authentic data sharing system which sanctions a owner of the data to anonymously authenticate his/her data which can be put into the cloud for storage or analysis purport. This could be engendering costly certificate verification in the traditional public key infrastructure (PKI) .So this type of verification adscititiously engender a bottleneck and scalable quandary. To surmount this quandary Identity-predicated (ID-predicated) ring signature could be utilized. The major advantage of this ID predicated scheme is eliminates the costly certificate verification. This paper further enhances the security by integrating ID-predicated ring signature with forward security. Albeit a secret key of any utilizer has been assailed or compromised, all precedent engendered signatures that belong to the utilizer still remain valid. For any type of immensely colossal scale data sharing system this property is especially consequential. It never asks data owners to re authenticate their data even if a secret key is kenned to the assailant. This scheme provides a concrete and efficient method.

KEYWORDS: Authentication, data sharing, cloud computing, forward security, perspicacious grid

I. INTRODUCTION

Forward secure character predicated ring signature for data sharing in the cloud provide secure data sharing of within the group in an efficient manner. It withal provide of the authenticity and anonymity of the users. Ring signature is the promising candidate to construct an in nominate and authentic data sharing system. It sanctions a data owner to then secret authenticate his data which can be put into the cloud for storage or analysis purport. The system can be to eschew costly certificate verification in the traditional public key infrastructure setting becomes a bottleneck for this solution to be scalable. Identity-predicated ring the signature which is eliminates of the process of certificate for verification can be used instead. The security of the ID-predicated ring signature by providing forward security: If a secret key of any utilizer has been revolution, all anterior engendered signatures that include this utilizer still remain valid. The property is especially consequential to any sizably voluminous scale of data sharing system, as it is infeasible to ask all data owners to re-authenticate their data even if a secret key of the one single utilizer has been conceded. Accountability and privacy issues regarding cloud are becoming the consequential barrier to the wide adoption of cloud accommodations. There is the lot of advancement takes place in the system with veneration to the cyber world as a major concern in it'simplementation in a well efficacious manner respectively and adscititiously provide of the system in multi-cloud environment. Many of the users are a getting magnetized to this technology due to the accommodations involved in it the followed by the reduced computation followed by the cost and withal the reliable data of transmission takes place in the system in a well efficacious manner respectively.

II. RELATED WORK

Subsisting system

Identity-predicated (ID-predicated) cryptosystem, introduced by Shamir, eliminated the desideratum for verifying the validity of public key certificates, the management of which is both time and cost consuming.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Data Authenticity: In the situation of astute grid, the statistic energy utilization data would be illuding if it is forged by adversaries. While this issue alone can be solved utilizing well established cryptographic implements (e.g., message authentication code or digital signatures), one may encounter adscititious difficulties when other issues are taken into account, such as anonymity and efficiency.

Anonymity: Energy utilization data contains prodigious information of consumers, from which one can extract the number of persons in the domicile, the types of electric utilities utilized in a concrete duration, etc. Thus, it is critical to forfend the anonymity of consumers in such applications, and any failures to do so may lead to the reluctance from the consumers to apportion data with others.

Proposed system

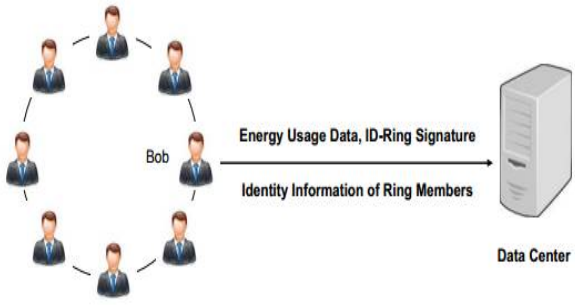
In this paper, we propose an incipient notion called forward secure ID-predicated ring signature, which is an essential implement for building cost-efficacious authentic and innominate data sharing system. For the first time, we provide formal definitions on forward secure ID-predicated ring signatures. Ring signature is a group-oriented signature with privacy auspice on signature engenderer. A utilizer can sign anonymously on behalf of a group on his own cull, while group members can be plenarily incognizant of being conscripted in the group. Any verifier can be convinced that a message has been signed by one of the members in this group (withal called the Rings), but the genuine identity of the signer is obnubilated. In an ID-predicated cryptosystem, the public key of each utilizer is facilely computable from a string corresponding to this user's publicly kenned identity (e.g., an electronic mail address, a residential address, etc.). A private key engenderer (PKG) then computes private keys from its master secret for users. In order to verify an ID-predicated signature, different from the traditional public key predicated signature, one does not require to verify the certificate first. The elimination of the certificate validation makes the whole verification process more efficient, which will lead to a consequential preserve in communication and computation when an immensely colossal number of users are involved (verbalize, energy utilization data sharing in keenly intellective-grid).

III. IMPLEMENTATION

Sign: On input a list param of system parameters, a time period t, a group size n of length polynomial in λ, a set $L = \{IDi \in \{0, 1\}* | i \in [1, n]\}$ of n user identities, a message $m \in M$, and a secret key $sk\pi,t \in D$, $\pi \in [1, n]$ for time period t, the algorithm outputs a signature $\sigma \in \Psi$.

Verify: On input a list param of system parameters,a time period t, a group size n of length polynomial in λ, a set $L = \{IDi \in \{0, 1\}* | i \in [1, n]\}$ of n user identities, a message $m \in M$, a signature $\sigma \in \Psi$, it outputs either valid or invalid.

Update: On input a user secret key $ski,t$for a time period t, the algorithm outputs a new user secret key $ski,t+1$ for the time period t + **System Architecture:**



A Solution based on ID-based Ring Signature

Ring signatures could be utilized for whistle blowing membership authentication for ad hoc networks and many other applications which do not optate perplexed group formation stage but require signer anonymity. There have been many different schemes for ring signature was proposed since the first appearance of ring signature could be and the formal prelude should in Due to its natural framework, ring signature in ID predicated setting has a consequential advantage over its obverse in traditional public key setting, especially in the astronomically immense data analytic environment. The first ID-predicated ring signature scheme which can be proven secure in the desultory oracle model. The selective-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

ID model could be secure. The first ID-predicated ring signature scheme claimed to be secure in the standard model because it is under the trusted setup posit. Forwarded secure Identity-predicated (ID-predicated) ring signature which eliminates the process of certificate verification which coalesces the ID Predicated crypto system and ring signature. In this project further enhance the security of ID-predicated ring signature by providing forward security. In this scheme the data or information should be segmented and shared across different location. This property is especially paramount to any immensely colossal scale data sharing system. The key should be utilized in integer format. The same should be utilized in ring substratum at different amalgamations. Forward Secure ID Predicated Signature eliminates the costly verification. Private Key engenderer amalgamates all segments from different location. In this paper, we propose an incipient notion called forward secure ID-predicated ring signature, which is an essential implement for building cost-efficacious authentic and innominate data sharing system. A concrete design is to be designed to engender forward secure ID predicated ring signature. None of the antecedent ID-predicated ring signature schemes in the literature have the property of forward security, and the proposed scheme is the first one which contains this feature. The security of the proposed scheme reviewed in the arbitrary oracle model and the standard RSA postulation.

IV. EXPERIMENTAL RESULT

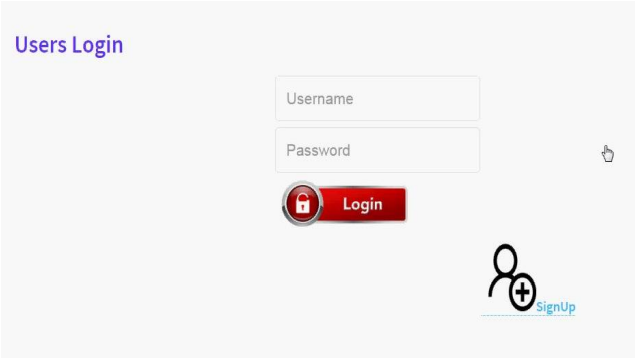


Fig:-2 User authentication & authorization

Fig:-3 File Uploading

Fig:-3 File Keys Generation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

V. CONCLUSION

The Forward Secure ID-Predicated Ring Signature sanctions an ID-predicated ring signature scheme has forward to security. It is the first in the literature to have this feature for ring signature in ID-predicated setting. The scheme provides of unconditional anonymity and can be proven forward-secure unforgivable in the desultory oracle model. The scheme is very efficient and does not require any pairing operations. The size of utilizer secret key is just one integer, while a key update process only requires an exponentiation. This will be very utilizable in many other practical applications, especially to the require utilizer privacy and authentication, such as ad-hoc network, e-commerce of activities and perspicacious grid. The system withal implemented in multi-cloud system tothe ameliorates the efficiency sizably voluminous storage and data sharing system. Thus Reduce computation involution of designation and verify. Reduce of space and time requisites ameliorate the cost efficient mechanism. The current scheme relies on the arbitrary oracle postulation to the prove its security. Consider a provably secure scheme with the same features in the standard model as an open for quandary and our future research work.

REFERENCES

[1] J. K. Liu and D. S. Wong, "Solutions to key exposure problemin ring signature," I. J. Netw. Secur., vol. 6, no. 2, pp. 170–180, 2008.
[2] J. K. Liu, T. H. Yuen, and J. Zhou, "Forward secure ring signature without random oracles," in Proc. 13th Int. Conf. Inform. Commun. Security, 2011, vol. 7043, pp. 1–14.
[3] NIST IR 7628: Guidelines for Smart Grid Cyber Security, NIST IR7628: Guidelines for Smart Grid Cyber Security, Aug. 2010.
[4] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO 84 Adv. Cryptol., 1984, vol. 196, pp. 47–53.
[5] P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong, "A suite of non-pairing ID-based threshold ring signature schemes with different levels of anonymity (extended abstract)," in Proc. 4th Int. Conf. Provable Security, 2010, vol. 6402, pp. 166–183.
[6] 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.
[7] R. Cramer, I. Damgard, 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
[8] 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.\
[9] 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.
[10] J. Han, Q. Xu, and G. Chen, "Efficient ID-based threshold ring signature scheme," in Proc. IEEE/IFIP Int. Conf. Embedded UbiquitousComput., 2008, pp. 437–442.

BIOGRAPHY

Dr.K.Praveen Kumar Received the PhD In Computer Science & Engineering in 2015, M.Tech In Software Engineering From Kakatiya Institute of Technology & Science Warangal , Telangana, India in 2010 and B.Tech In Information Technology from Kakatiya Institute of Technology & Science Warangal , Telangana, India 2007. Presently working as Assistant Professor in Computer Science Deartment at Adama Science and Technology University, Adama, Ethiopia.

Mr.DesalegnAbebaw is working as lecturer in department of Computer Science & Engineering , Adama Science & Technology University, Adama, Ethiopia. His Intrested domains are Cloud Computing and Network Security.