Forward Secure ID Based Ring Signature For Data Sharing

Swati Khatal
Dept of Computer
Terna Engineering College, Maharashtra, India

Abstract- *Cloud computing provides services wherever one will access data from anyplace, from anyplace, at any time. thus primarily, cloud computing is subscription-based service wherever one will get network space for storing and pc resources for information storage likewise as information sharing. because of high fame of cloud for information storage and sharing, sizable number of participants gets drawn to it. the safety is that the biggest concern for adoption of cloud. the foremost problems during this regard area unit potency, information integrity, privacy and authentication. so as to handle these problems conception of ring signature has been introduced for information sharing amongst sizable number of users. Ring signatures area unit want to give user's namelessness and signer's privacy. however, the pricey certificate verification within the ancient public key infrastructure (PKI) setting becomes a bottleneck for this answer to be scalable .ID primarily based ring signature had been introduced that eliminates the method of certificate verification. more sweetening of security with forward security conception has been introduced. in step with this idea, if a secret key of any user has been compromised; all previous generated signatures that embrace this user still stay valid. This property is very necessary to any large-scale information sharing system, because it is not possible to raise all information house owners to re-authenticate their information albeit a secret key of 1 single user has been compromised. Thus, we tend to propose secure ID primarily based ring signature with forward security.*

Keywords- Authentication, data sharing, cloud computing, forward security

I. INTRODUCTION

The popularity and hyperbolic use of cloud makes information sharing additional convenient. information sharing provided supplemental advantages to society.

Example: Consumers in smart Grid will acquire their energy usage information in a very fine-grained manner and are inspired to share their personal energy usage information with others like by uploading the info to a third-party platform like Microsoft Hohm. From the collected information a applied mathematics report is made, and one will compare their energy consumption with others (e.g., from identical block). This ability to access, analyze, and answer far more precise and careful information from all levels of the electrical grid is essential to economical energy usage.

There are several security goals a practical system must meet like

Data Authenticity: In the scenario of smart grid, the data point energy usage information would be dishonorable if it's solid by adversaries. whereas this issue alone is solved exploitation well established cryptanalytic tools (e.g., message authentication code or digital signatures)

Anonymity: Energy usage data contains vast information of consumer

Energy usage knowledge contains large data of client from that one will extract the quantity of persons within the home, the kinds of electrical utilities utilized in a particular fundamental quantity, etc. Thus, it's important to shield the namelessness of shoppers in such applications, and any failures to try to to therefore might cause the reluctance from the shoppers to share knowledge with others and

Efficiency: the quantity of users during a knowledge sharing system can be immense and a sensible system should cut back the computation and communication value the maximum amount as potential. Otherwise, it might cause a waste of energy, that contradicts the goal of smart grid.

We propose "identity-based ring signature" which is an efficient solution on applications requiring data authenticity and anonymity and security. It is further strengthened by adding forward security to it.

APPLICATIONS OF FORWARD SECURE ID-BASED RING SIGNATURES:

Smart Grid: Smart Grid is one type of electricity network that has digital technology. The good grid has two-way capabilities for knowledge communication: Not solely the grid controller

will issue commands to intelligent devices, shoppers and devices may also send knowledge to grid controllers. the flexibility to access, analyze, and reply to far more precise and elaborate knowledge from all levels of the electrical grid is important to the key advantages of the good Grid. As AN example, Microsoft Hohm provides a platform for shoppers to transfer energy usage knowledge, supported that a applied math report is formed. the aim is to encourage shoppers to match their energy consumption with others (e.g., on an equivalent street) and so use electricity additional with efficiency. knowledge integrity may be a necessary demand in those applications since the comparison would be insignificant if the info is maliciously changed or faked. Privacy, on the opposite hand, is additionally a big concern: shoppers might not need to administer their identity info to any third-party service suppliers. Ring signature may be a promising answer on applications (e.g., Microsoft Hohm) requiring each integrity and privacy. In ring signature, a sound signature can persuade the service supplier that the info is uploaded by a shopper on a definite street, while not telling World Health Organization precisely the shopper is. Forward security is actually fascinating during this state of affairs since a compromised personal key inside a fundamental measure won't have any negative impact on applied math reports generated antecedently. In alternative words, recent applied math reports would stay valid if forward-security is satisfied.

Whistle Blowing: Suppose in some corporate sector if employee want to register complaint regarding higher authority or anyone else they can use forward secure id based ring signature to anonymously send message to concern person. The admin can verify that message is from authorized person only though he can't understand who the actual signer is. Forward security enhances the protection of all entities. Without forward security, if a secret key of member is exposed, every ring signature containing that member in the ring will become invalid. This will greatly affect the accuracy of the information

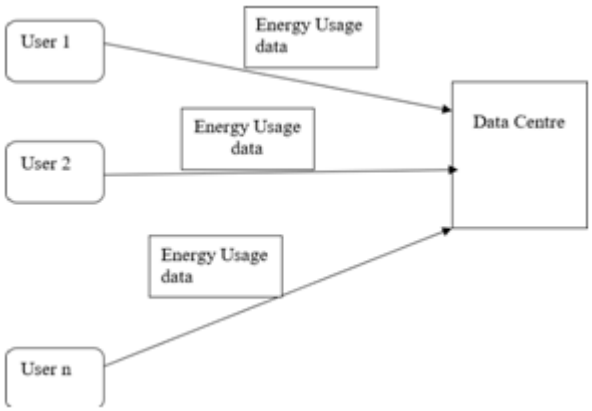

Fig: Energy usage data sharing in smart grid

The rest of the paper is formulated as Section 2 briefs the literature survey that covers some existing Ring Signature schemes. The proposed methodology and algorithm are demonstrated in section 3. Section 4 briefs about the experimental results. Finally, in Section 5 the conclusion is presented.

II. LITERATURE SURVEY

There are several literatures on different ring signature schemes. Sub-linear size ring signature scheme produces ring of group of users, which includes the signer. In this ring signature scheme that has size O (√N) where N is the number of users in the ring. An additional feature of scheme is that it has perfect anonymity. Though it provides anonymous authentication but it needs costly public key certificate verification. To overcome this issue ID-based Ring Signature from Pairings scheme enables a signer in an ad hoc manner to sign a signature on behalf of a group of users including him such that a verifier can be convinced that one of the identified users actually generated the signature but he cannot identify the actual signer. Though it avoids public key certificate verification but key exposure problem occurred. To make ring signature more efficient Non-pairing ID based threshold ring signature scheme does not have any bilinear pairing. As it is ID based, it avoids public key certificate verification but key exposure problem occurred. According to need in different application some other types of ring signatures were proposed. In Linkable ring signature identity of the signer in a ring signature remains anonymous, but two ring signatures can be linked if they are signed by the same signer. Length of the signature depends on the number of members. Blind Ring Signature Scheme can provide the anonymity of the signed message; thus, it can realize the private protection of user's transaction information. But the length of the signature depends on the number of members. Thus, it is an open problem to construct a blind ring signature with constant size. To overcome the problem of size of ring signature ID-Based Ring Signature

Scheme with Constant-Size Signature scheme the size of ring signature depends linearly on the ring size. Also, it was having many security issues. Threshold ring signature scheme based on coding. Ring signature is one type of group-oriented signature with privacy protection on each user. A user can sign individually on behalf of a group of his own choice and send to the other persons in the group. It protects the system from attack of ring member change.

III. METHODOLOGY

The SHA256 algorithm is used to generate Hash of public key. We assume that the identities and user secret keys are valid into T periods and make the time intervals public. We also set the message space M= {0,1}*.

The following algorithms are used for the ID based ring signature and verification.

Setup: On input of a security parameter λ, the PKG generates two random k-bit prime numbers p and q such that p=2p'+1 and q=2q'+1 where p',q' are some primes.

It computes N =pq. For some fixed parameter l , it chooses a random prime number e such that 2l<e<2l+1 and gcd(e, ϕ(N)).

It chooses two hash functions H1:{0,1}*→ Z*N and H2:{0,1}*→{0,1}. The public parameters are (k,l,e,N,H1,H2) and the master secret key msk is (p, q).

Extract: For user i, where i Z, with identity IDi {0,1}* requests for a secret key at time period (denoted by an integer), where 0 ≤t < T, the PKG computes the user secret key
Ski,t=[H1(IDi)]1/e(i+1-1) mod N Using its knowledge of the factorization of N.

Update: On input a secret key sk i,t for a time period t, if t < T the user updates the secret key as
Ski,t+1 = (ski,t)e mod N
Otherwise, the algorithm outputs meaning that the secret key has expired.

Sign: To sign a message m {0,1}* in time period t, where 0≤t < T, on behalf of a ring of identities L = {ID1,….,IDn}, a user with identity ID . Land secret key sk t: 1)For all i{1,…..n},i#, choose random
Ri=Ai e(x+1-t) mod N and hi = H2(L,m,t.ID, Ri)

2) Choose random A π=Z*N and compute:

$$R\pi = A\pi\text{^}e(T + 1 - t)$$

Π H1(IDi)-hi mod N And
h =H2(L,m,t,ID)
3) Compute s= (sk π,t)h Πni=1 Ai mod N.
4) Output the signature for the list of identities L, the message m, and the time period t as

σ = (R1,…..,Rn,h1,….,hn,s)

AES algorithm is used to encrypt the data while saving the message in database to make it more secure.

Verify: To verify a signature for a message m, a list tf identities L and the time period t, check whether hi = H2 (L,m,t,IDi,Ri) for i=1,…, n and
Se(T+1-t) = Πni=1(Ri. H1(IDi)hi) mod N
Output valid if all equalities hold otherwise output invalid..

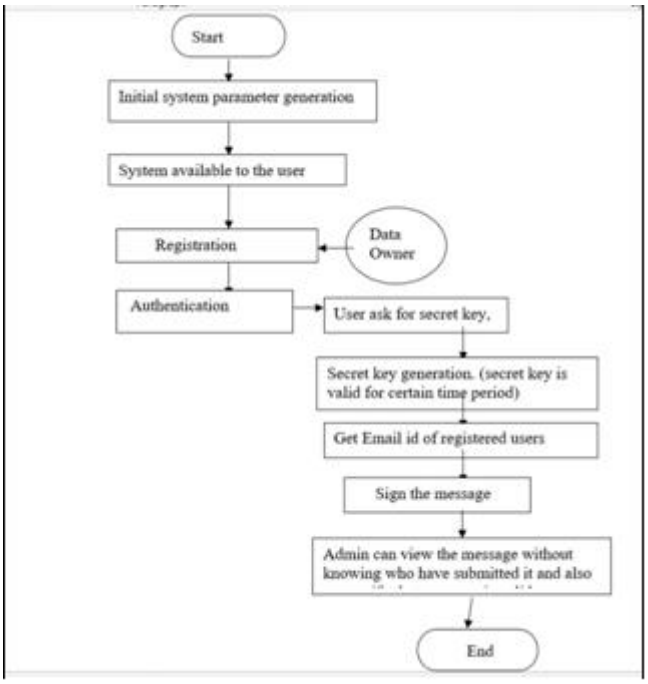

Fig: System Flow Chart

IV. EXPERIMENTAL RESULT

The time for the data owner to sign data by using key generated by MD5

We have analyzed the time required for signing data by secret key of ring user which is generated by MD5 and SHA256

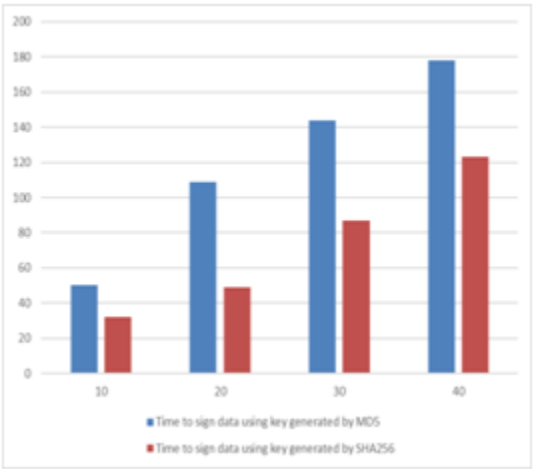

Figure: Graphical representation of time required to sign data by using key generated from MD5 and SHA256

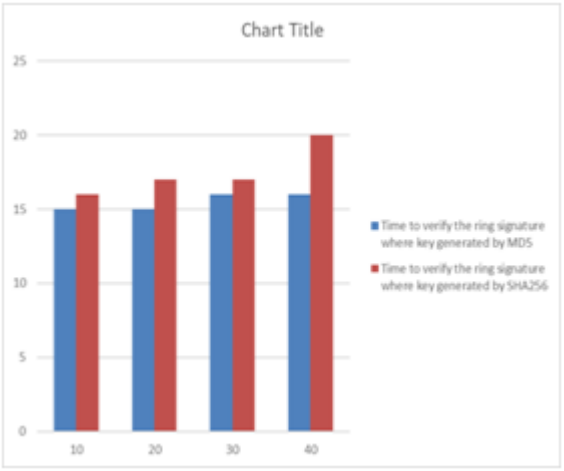

Figure: Graphical representation of the time required for the service provider to verify the ring signature where key generated by MD5 and SHA256

V. CONCLUSION

Data sharing systems offer associate economical method for user to exchange the knowledge open the general public network. Despite of varied benefits the safety problems area unit the foremost obstacle for its adoption. The necessary problems which require to be addressed area unit knowledge integrity, privacy and potency. the varied schemes area unit gift in literature however none of them is totally secure. In this work a Forward secure ID-based ring signature scheme is proposed to ensure the security of data shared over the network. The scheme can provide unconditional anonymity along with security to the user's data.

ID based ring signature provides group signature with anonymity and time constraints which proves concept of forward security. Also public key certificate verification is not necessary which gives efficient and cost effective solution to the problem.

This scheme will be very useful in many other practical applications, especially in ad-hoc network, whistle blowing, e-commerce activities and smart grid.

REFERENCES

[1] 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

[2] N. Chandran, J. Groth, and A. Sahai, "Ring signatures of sub linear size without random oracles," in Proc. 34th Int. Colloq. Automata, Lang. Programming, 2007, vol. 4596, pp. 423–434

[3] 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

[4] 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.

[5] 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

[6] 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

[7] 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

[8] 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.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO 84 Adv. Cryptol., 1984, vol. 196, pp. 47–53.

[10] J. Yu, F. Kong, H. Zhao, X. Cheng, R. Hao, and X.-F. Guo, "Non-interactive forward-secure threshold signature without random oracles," J. Inform. Sci. Eng., vol. 28, no. 3, pp. 571–586, 2012.

[11] 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.

[12] 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.

[13] 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

[14] T. H. Yuen, J. K. Liu, X. Huang, M. H. Au, W. Susilo, and J. Zhou "Forward secure attribute-based signatures," in Proc. 14th Int. Conf. Inform. Commun. Security, 2012, vol. 7618, pp. 167–177.

[15] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.