International Journal For Technological Research In Engineering
Volume 4, Issue 2, October-2016 *ISSN (Online): 2347 - 4718*

RELIABLE AND SECURE DATA SHARING WITH FORWARD SECURITY IN CLOUD ENVIRONMENTS

Kallukunta Sekhar[1], M. Anand[2]
[1]PG Scholar, [2]Assistant Professor
Dept of CSE, Bheema Institute of Technology and Science, Adoni, Kurnool (Dt), AP, India

Abstract: Due to the advance of recent technology data sharing has never been easier in this world an accurate analysis on the shared data provides a bunch of benefits to both the society and people. Data sharing between two members or cluster of members should take into consideration several issues they are efficiency, data integrity and privacy of data owner to overcome this issue Ring signature plan is introduced. it is a promising approach to construct a secret and authentic data sharing system that allows a owner of the data to anonymously authenticate his/her data which might be place into the cloud for storage or analysis purpose. this may be making costly certificate verification within the public key thus this type of verification additionally produce a bottleneck and scalable drawback to overcome this drawback Identity-based (ID-based)ring signature may be used the major advantage of this ID based scheme is ignore the costly certificate verification. This paper more enhances the protection by integration ID-based ring signature with forward security though a secret key of any user has been attacked or compromised, all previous generated key signatures that belong to the user still remain valid. For any reasonably large scale data sharing system this property is especially necessary. It never asks data owners to re-authenticate their information though an unknown key is familiar to the attacker. This theme provides a concrete and economical methodology.

Index Terms: Cloud Computing, Ring Signature Scheme, Forward Security;

I. INTRODUCTION

In cloud computing, there are variety of security issues/concerns related to cloud computing however these issues fall under two broad categories: security issues faced by cloud worker and security issues faced by their The responsibility goes both ways, however: the provider should guarantee that their infrastructure is secure which their clients' data and applications are protected whereas the user should take measures to fortify their application and use robust passwords and authentication .The popularity and wide-spread make use of cloud has brought great convenience for data sharing and collection. Not only can individuals acquire useful data lots of simply, sharing data with others can provide variety of advantages to our society moreover as a representative example, customers in Grid. Will get their energy usage data in a fine-grained manner and are impressed to share their personal energy usage info with others, for example by uploading the data to a third party platform like Microsoft Ohm. From the collected data a statistical report is formed, and one can compare their energy consumption with others for example from constant block. This ability to access, analyze, and answer a lot of a lot of precise and detailed data from all levels of the electrical grid is important to efficient energy usage. Due to its openness, data sharing is sometimes deployed in a hostile atmosphere and vulnerable to variety of security threats .Taking energy usage data sharing of security menaces. Sharing in smart Grid as an example, there are several security goals in practice they are: 1) Reliability of data: the situation of Grid, the statistic energy usage data being deceptive if it is cast by adversaries. Whereas these issues alone are resolved using well established cryptographic tools, one might encounter more difficulties once different issues are taken into thought, like namelessness and talent. 2) Un-singularity: Energy usage data contains huge data of customers, from that summary the quantity of persons within the home, sort of electrical utilities utilized in a selected amount of time it is important to safeguard the anonymous consumers applications, and any failures to try to thus may result in the reluctance from the client to share data with others. 3) Effectiveness: the various users throughout a data sharing System might be huge and a smart system should cut back. The computation and communication worth the most amount as possible. Otherwise it might result in a waste of energy that contradicts the goal of Grid. To investigating basic security tools for realizing the three properties we tend to delineated. Note that there are alternative security issues throughout a data sharing system that are equally necessary, like convenience and access management. In a very ring signature theme the key exposure produce extra severe drawback. If the secret key of one of the ring member's is exposed by the attacker means that they will turn out valid ring signatures of any documents happiness to it cluster. For doing this sort of attack the attacker only needs to include the compromised user within the "group" and mutely watch the operation between the teams. The exposure of one user's secret key might discover all previously obtained ring signature however the condition is that user is one amongst the ring member's. Since the member cannot identify whether a ring signature is generated previous to the key exposure or not without using any mechanism so the forward security is also a necessary demand throughout a large data sharing system. Otherwise, large quantity of time and resource are waste. The forward-protected digital signatures ought to be designed in numerous fashions so as to feature forward security on ring signature two varieties forward protected ring signature schemes however they every add the normal universal key setting. During this type of settings the

signature verification involves costly certificate check for each ring member. This may work for large ring conjointly just like the lot of range of users in a very smart grid. So as to summarize the development of ID-based ring signature with forward security and it is a basic tool. The key options of this forward security theme are its elimination of the pricey certificate verification methodology makes it scalable for large number of users and particularly applicable for big data analytic setting. The scale of a secret key is only one integer. Key update method only needs an operation time. The pairing operation couldn't be utilized in any stage.

II. RELATED WORK

In cipher, a ring signature is a kind of digital signature which will be performed by any member of a bunch of users that every have keys. Therefore, a message validate with a ring signature is supported by someone in a specific cluster of people. One among the security properties of a ring signature is that it ought to be computationally not possible to see that of the cluster member's keys was used to produce the signature. Ring signatures are kind of like cluster signatures however dissent in two key ways: initial, there is no way to revoke the anonymity of an individual signature, and second, any cluster of users is used as a gaggle while not further setup. Ring signatures were invented by Ron Rivest, Adie Shamir, and Yael Tauman, and introduced within the name "ring signature" comes from the ring-like structure of the signature rule. Ring signatures contains only two algorithms: Sign and Verify; this encapsulates the intuition that ring signatures are primarily "setup-free" (i.e. don't would like the Key generation algorithm) and categorically unidentified .In more recently planned ring signature schemes, however, a Key generation algorithm has been extra as the way to ensure that each one users have the same reasonably keys. Therefore, for the needs of security definitions we assume that a digital signature theme consists of various algorithms: Key generation, Sign, and Verify. Every user can run Key generation individually; this rule, on input the protection parameter 1k, can output a key combine (pk,sk). The Sign rule, on input a secret key sk, a ring R (typically merely a listing of public keys happiness to members of the ring), and a message "m", and an outputs a signature "σ" on m. finally, the validate rule, on input the ring R, a signature σ, and a message m1, outputs one if some member of R created the signature σ on m and 0 otherwise by instinct, we would like ring signatures to be secure in ways in which almost like cluster signatures. It turns out we are able to succeed an anonymity notion but whereas not a Trace algorithm we clearly cannot hope to achieve one thing that seems like traceability. We might still wish to ensure that non-ring members cannot forge signatures, then we tend to instead think about the marginally weaker property of enforceability every these properties were initial outlined formally by Bender, Katz, and Morselli. As outlined by Bender et al., there are three potential levels of anonymity we can achieve: basic anonymity, within that which the individual sees only public keys; anonymity with relevance adversarial chosen keys, within which the individual (as the name implies) can opt for its own key pairs and then primarily produce its own users; and finally, anonymity with regard to full key exposure, within which the individual will still opt for its own key pairs but to boot gets to envision the key keys for each user. Data sharing with an oversized kind of participants should take into thought several issues, in addition as efficiency, data integrity and privacy of data owner. The flexibility to access, and answer rather more precise and elaborate data from all levels of the electrical grid is vital to optimum energy usage. Because of its openness, data sharing is sometimes deployed in an open environment and weakness to kind of security threats. If user need to revoke from the cluster it's impossible in my system.1) it is difficult to provide security.2) it is important to economical energy usage.3) data integrity is low.4) User data tell others. User cannot be a part of completely different cluster, if he/she is member of any cluster there is no revocation manager this result in unconditional anonymity of signer.

III. FRAME WORK

In this proposed system, we projected an ID-based ring signature scheme with forward security. We also known as forward secure ID-based ring signature scheme. In this system the Forward security identification-based (identity-based) ring signature which eliminates the strategy of certificate verification which combines the id based crypto approach and ring signature. On this challenge extra increase the safety of identification-based ring signature by using providing forward security. During this theme the data or information can got to be segmented and shared across unique area. This property is especially to any massive scale data sharing methodology. The vital issue should be used in integer layout. The identical should be employed in ring foundation at exceptional mixtures. Ahead relaxed identification established Signature eliminates the certificate verification. Private Key generator combines all segments from distinctive location. During this paper, we propose a novel inspiration known forward secure ID-based ring signature, that is associate essential instrument for constructing cost-robust respectable and unknown data sharing methodology. A concrete style is to be designed to form forward secure identity based ring signature. None of the previous identification-based ring signature schemes inside the literature have the property of forward safety, and the planned scheme is that the initial one which contains this feature. The protection of the planned scheme reviewed within the random oracle model and the usual RSA assumption.

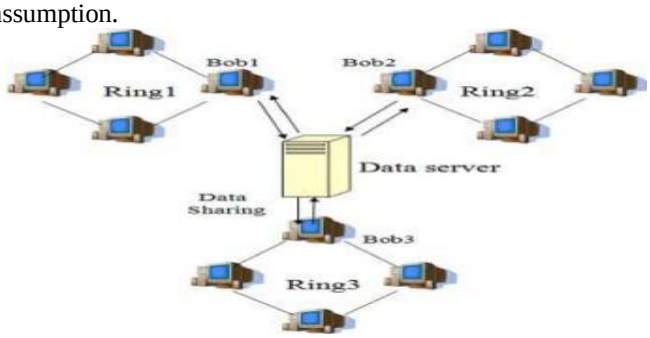
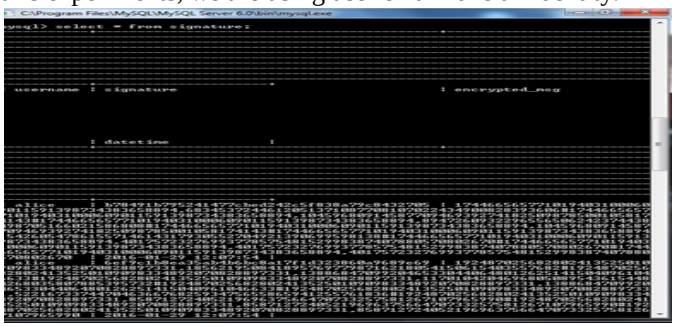


Figure 1: System Architecture

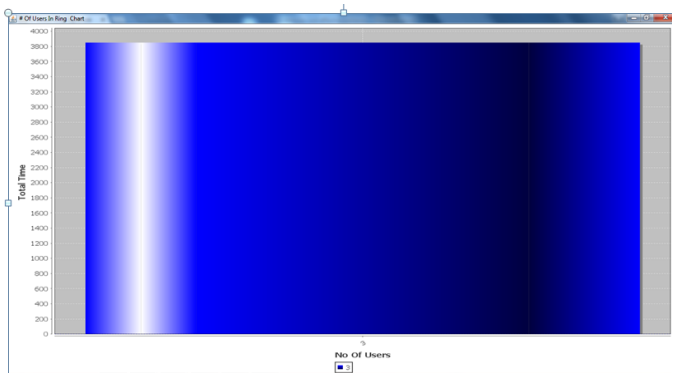
ID-based Ring Signature: in a ring signature format, a user signs a message secretly on behalf of a group (or ring) of users which consists himself. This group is not fixed, but selected ad hoc by the actual signer just before computing the signature. The verifier is influenced that some member of the ring has signed, however he does not have any data about who the real signer is. Ring signature provides anonymous as well as legitimate data sharing. Identification based mostly ring signature eliminates the need of certificate verification thus presents cost effective resolution. Forward Security: In cryptography, forward security could be possessions of secure communication protocols during which cooperation of long-term keys does not cooperation past session keys. Forward security protects past sessions aligned with future compromises of secret keys otherwise passwords. By using this proposed scheme we eliminate the certificate verification process. This projected system is very helpful for user authentication furthermore as security. From our experiments, we proved that our projected scheme is very economical as well a scalable scheme.

IV. EXPERIMENTAL RESULTS

In our experiments, any number of users can registered and login into the system. Authorized user can add and generate the group signature user can select the building size for example: number of rooms, and electronic items i.e. number of items and enter the energy consumption of the building and that information is saved in database to shown in below screen and that information is visible to all registered authorized users if unauthorized user can see the information that information not visible. Here, the signatures will be created for the submitted data and the access permissions are created by using Identity-based (ID-based) ring signature in this experiments, we are using user email id is an identity.



In the below chart we can observe that ring generation time chart



We can observe that ring based signature generation time chart. The data will also available for certain time slot if we are try to checking the data after a month user is unable to view the information as the time is expired and user view the information within limited amount of time. Then the system displays the alert like "time expired". Through our implementation we have implemented an efficient system to create and generate the group by using ID-Base ring signature and eliminate the costly certificate verification and store the data in encryption format so we can consider that store the data in secure format and reduce the cost then compare to current system.

V. CONCLUSION

In this paper, we proposed an ID-based ring signature scheme with forward security. We also called as forward secure ID-based ring signature scheme. It allows an ID-based ring signature theme to have forward security. It is the first in the prose to have this characteristic for ring signature in ID-based setting. Our theme provides unconditional anonymity and should be tried forward-secure unforgivable within the random oracle model, assumptive RSA drawback is difficult. Our theme is extremely efficient and doesn't want any pairing operations. The scale of user secret is simply one integer, whereas the key update methodology solely needs an operation. we have a tendency to believe our theme are very useful in several different wise applications, particularly to those need user privacy and authentication, like ad-hoc network, smart grid and ecommerce activities. Our current theme depends on the random oracle assumption to prove its security to enhance the security for authentication on ring members using Mac algorithm. SHA-1 and MD5 algorithm is used for data cryptography throughout this algorithm is used for large size of data should be encrypted, Sharing data on one ring members to different ring members. Then enhance security on data sharing and transfer the data on cloud.

REFERENCES

[1] M.H .Au, J.K. Liu, T.H. Yuen, and D.S. Wong. Id-based ring signature scheme secure in the standard model. In IWSEC, volume 4266 of Lecture Notes in Computer Science, pages 1–16. Springer, 2006.

[2] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau. Security and privacy enhancing multi cloud architectures. IEEE Trans. Dependable Sec.Comput. 10(4):212–224, 2013.

[3] 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.

[4] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong. Id-based ring signature scheme secure in the standard model. In IWSEC, volume 4266 of Lecture Notes in Computer Science, pages 1–16. Springer, 2006.

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

[6] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of group signatures: formal definitions, simplified requirements and a construction based on generalassumptions.InEUROCRYPT'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 Computer Science, pages 431–448. Springer-Verlag, 199

[8] J. K. Liu, V. K. Wei, and D. S. Wong. A separable threshold ring signature scheme. In ICISC, volume 2971 of Lecture Notes in Computer Science, pages12–26.Springer, 2003.

[9] J. K. Liu and D. S. Wong. On the Security Models of (Threshold) Ring Signature Schemes. In ICISC 2004, Lecture Notes in Computer Science. Springer, 2004.

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

[11] J. K. Liu, T. H. Yuen, and J. Zhou. Forward secure ring signature without random oracles. In ICICS, volume 7043 of Lecture Notes in Computer Science, pages 1–14. Springer, 2011.

[12] A. L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen. Practical short signature batch verification. In CT-RSA, volume 5473 of Lecture Notes in Computer Science, pages 309–324. Springer, 2009.Full version appeared in http://eprint.iacr.org/2008/015.

[13] J. Han, Q. Xu, and G. Chen. Efficient id-based threshold ring signature scheme. In EUC (2), pages 437–442. IEEE Computer Society, 2008.

[14] J. Herranz. Identity-based ring signatures from RSA, Theor. Comput. Sci., 389(1-2):100–117, 2007.

[15] J. Herranz and G. Sáez. Forking Lemmas for Ring Signature Schemes. In T. Johansson and S. Maitra, editors, INDOCRYPT 2003, volume 2904 of Lecture Notes in Computer Science, pages 266–279. Springer, 2003.

[16] M. Klonowski, L. Krzywiecki, M. Kutylowski, and A. Lauks. Stepout ring signatures. In MFCS, volume 5162 of Lecture Notes in Computer Science, pages 431–442. Springer, 2008.

