International Journal For Technological Research In Engineering
Volume 5, Issue 1, September-2017 *ISSN (Online): 2347 - 4718*

IMPROVING SECURITY AND ELIMINATING CERTIFICATE VERIFICATION PROCESS BY IMPLEMENTING FORWARD SECURITY IN CLOUD COMPUTING

D. Sivasri[1], S. Bhaskara Rao[2]
[1]PG Scholar, [2]Assistant Professor, Dept of CSE, Sri Venkateswara College of Engineering and Technology, Etcherla, Srikakulam (Dt), AP, India.

ABSTRACT: ***Every day we are sharing huge amount of data in cloud computing. While data sharing among the cloud users, they*** **are face huge amount of issues like,** ***authentication, cost, time in uploading and many other criterions. Authentication of data is have got to for utilizing the others data and importing our own information has come to be tedious. Getting certificates and for each access is lengthy procedure and price increases. Ring signature gives an assurance to the consumer to construct an unidentified and correct knowledge sharing procedure. It makes it possible for knowledge individualistic to in nominate authenticate his knowledge which can also be put into the cloud for storage or evaluation rationale. In identity-based (ID-based) Ring Signature contributors of this cluster can with ease share knowledge warding off the high-priced certificates verification as done within the natural method. To improve the security of the ID-based Ring Signature, in this paper we propose forward security and this Forward Security concept used in large scale data sharing systems.***

I. INTRODUCTION

Cloud Computing is uninterrupted growing latest technology in IT trade, academe and business. The follow of employing a system of remote servers hosted on the web to store, manage, and method information, instead of a local server or a private computer. Cloud computing is very accessible, versatile technology that puts hardware, software, and virtualized resources. Cloud computing infrastructure mechanism over the web on demand basis; main options of cloud computing is that on-demand possibilities, broad network access, resource pooling, fast physical property ,measured service measurability and offers shared services to user on demand basis in distributed atmosphere. Ordinarily accessible cloud computing service suppliers are Google, Yahoo, Microsoft, Amazon etc. the details of cloud services are abstracted from users. The foremost common problems with cloud computing are as potency, integrity and authenticity. Moreover, users are unaware of location wherever machines that truly method and host their information. Ring signature for knowledge sharing within the cloud give secure knowledge sharing exploitation forward secure identity primarily based inside the cluster is performed in secure manner. It conjointly gives the believability and anonymity of the top users. Ring signature may be a promising candidate to construct an anonymous and authentic knowledge sharing system for user. It permits a knowledge owner to on the Q.T. attest his data which might be place into the cloud for storage. The planned system avoids pricey certificate keys for verification within the ancient public key infrastructure setting becomes a bottleneck for this resolution to be ascendible. Identity-based ring signature that removes the method of certificate verification is used centered for future use and therefore the security of ID-based ring signature by offering forward security. If a secret key of any user has been leaked, all previous generated signatures that embrace this user still stay valid. The property is particularly vital to any massive scale knowledge sharing system, because it is not possible to raise all knowledge owners to re-authenticate their knowledge even though a secret key of 1 single user has been reveal. Answerableness and privacy problems concerning cloud have become vital issues for cloud services. There's tons of advancement takes place within the system with reference to the net as a significant concern in its implementation in an exceedingly well effective manner severally and conjointly give the system in multi-cloud atmosphere. Several of the users have gotten interested in this technology because of the services concerned in it followed by the reduced computation value and conjointly the reliable knowledge transmission takes place within the system in an exceedingly well effective manner severally. In a ring signature theme the key exposure produce a lot of severe drawback. If the key of one of the ring member's is exposed by the attacker suggests that they will turn out valid ring signatures of any documents belonging to it cluster. For doing this kind of attack the attacker solely must include the compromised user within the "group" and silently watch the group action between the teams. Since the member cannot establish whether or not a ring signature is generated before the key exposure or not while not victimization any mechanism. Therefore the forward security may be a necessary demand during a massive knowledge sharing system. Otherwise, large quantity of time and resource are going to be waste. The forward-secure digital signatures ought to be designed in varied fashions so as to feature forward security on ring signature. But they each add the normal public key setting. During this variety of settings the signature verification involves pricey certificate check for each ring member. This may work for large ring additionally admire a lot of range of users during a good grid. So as to summarize the planning of ID-based ring signature with forward security the forward security is that the elementary tool.

II. RELATED WORK

Javier Herranz IIIA, "Bellaterra, Spain identification-predicated cryptosystems do away with the desideratum for validity checking of the certificates and the desideratum for registering for a certificate for getting the general public key. These two aspects are fascinating specifically for the efficiency and the professional spontaneity of the ring signature, where a utilized can anonymously sign a message on behalf of a bunch of spontaneously conscripted customers including the authentic signer. The identity-predicated ring signature and dispensed ring signature schemes involve many public keys; it's mainly interesting to don't forget an identification-predicated construction which evades the administration of many digital certificates. A paramount property of the scheme is moreover formally provided and analyzed: opening the anonymity of a signature is possible when the official author wishes to take action. The security of all of the considered schemes will also be formally proved within the desultory oracle mannequin. The security of identity-predicated signature schemes is formalized with the aid of on account that essentially the most full of life viable kind of assaults.

C. A. Melchor, et al proposes a brand new effective threshold ring signature scheme headquartered on coding idea. Ring signature is a gaggle-oriented signature with privacy preserving on signature producer. A consumer can signal anonymously on behalf of a gaggle on his alternative and send to the opposite individuals within the workforce. Any verifier can also be convinced that a message has been signed with the aid of some of the members on this workforce (also known as the Rings), but the genuine identification of the signer is hidden. Ring signatures would be used for a whistle blowing anonymous membership authentication for advert hoc agencies and plenty of other applications which are not looking for tricky workforce formation stage however require signer anonymity.

MihirBellare and Sara K. Miner offered "A forward-secure Digital Signature Scheme". Digital signature scheme in which the public keys fine-tuned but the secret signing secret is updated at customary intervals so that you could furnish a head protection property: compromise of the present secret key does no longer permit an adversary to forge signatures bearing on the prior. This can be used to decrease the damage triggered with the aid of key publicity without requiring distribution of keys. The construction makes use of conceptions from the signature schemes, and is demonstrated to be forward secured predicated on the inflexibility of factoring, in the arbitrary oracle model. The construction is additionally rather effective. Past signature remain secure even though expose the present secret key.

III. FRAMEWORK

A. System Framework

Forward security identification-based (identity-based) ring signature which eliminates the method of certificate verification which combines the id headquartered crypto approach and ring signature. On this challenge additional increase the safety of identification-based ring signature by using providing forward security.

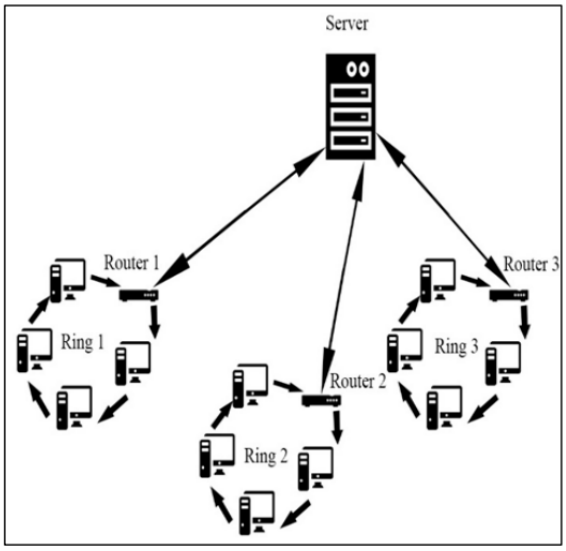


Fig 1. System Framework

In this scheme the information or information will have to be segmented and shared across unique area. This property is especially to any large scale data sharing method. The important thing should be used in integer layout. The identical must be used in ring foundation at exceptional mixtures. Ahead relaxed identification established Signature eliminates the certificate verification. Private Key generator combines all segments from distinctive location. In this paper, we propose a brand new inspiration known forward secure ID-based ring signature, which is an essential instrument for constructing cost-robust respectable and nameless information sharing method. A concrete design is to be designed to create forward secure identity based ring signature. The protection of the proposed scheme reviewed within the random oracle model and the usual RSA assumption;

ID-based Ring Signature

In a ring signature format, a user signs a message anonymously 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, but he does not have any knowledge about who the real signer is. Ring signature provides anonymous as well as legitimate knowledge sharing. Identification based ring signature eliminates the necessity of certificate verification hence presents cost effective solution.

Forward Security

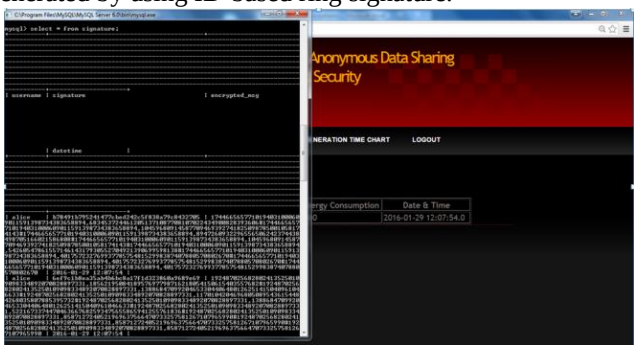
In cryptography, forward security is a possessions of secure communication protocols in which cooperation of long-term keys does not cooperation past session keys. Forward secrecy protects past sessions against future compromises of secret keys otherwise passwords.

B. Advantages of Proposed System

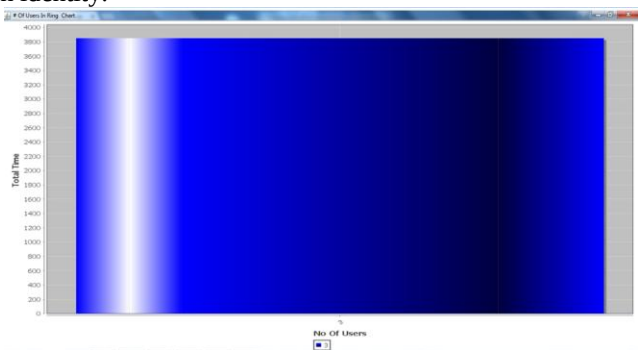
- Improved the scalability and flexibility are.
- Provide protection in information sharing
- Improved security and cost effective
- The safety of the proposed scheme is extended by utilizing this random oracle model.

IV. EXPERIMENTAL RESULTS

In our experiments, after login, user must add and generate the group signature. To generate group signature he needs to add some details like, username, building size, electronic items and energy consumption details. And the user stores those details in the system. When we are add the details then the signatures will be generated for the stored details which are inside the database. The access permissions are also generated by using ID-based ring signature.



The above screen shows that the generated signatures for saved data. In this experiments, we are using user email id is an identity.



The above screen shows that the ring based signature generation time chart. Here, the submitted data can be viewed by all registered user but it have some time limit. Such that if any registered user tries to view the data after time expiry then the system displays the alert like "time expired".

From our experiments, we proved that our proposed scheme is very efficient and scalable scheme.

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. By using this proposed scheme we eliminate the certificate verification process. This proposed system is very useful for user authentication as well as security. From our experiments, we proved that our proposed scheme is very efficient as well as scalable scheme.

REFERENCES

[1] M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n Signatures from a Variety of Keys. In ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 415–432. Springer, 2002.

[2] R. Anderson. Two remarks on public-key cryptology. Manuscript, Sep. 2000. Relevant material presented by the author in an invited lecture at the Fourth ACM Conference on Computer and Communications Security, 1997.

[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] 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 general assumptions. In EUROCRYPT'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, 1999.

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

[9] Boldyreva. Efficient Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap Diffie-Hellman Group Signature Scheme. In PKC'03, volume 567 of Lecture Notes in Computer Science, pages 31–46. Springer, 2003.

[10] D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. In CRYPTO 2004, volume 3152 of Lecture Notes in Computer Science, pages 41–55. Springer, 2004.

