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 6, June 2016

A Survey on Cost Efficient Authentic Mechanism for Sharing Data on Cloud

Pritee Raut[1], S.B.Natikar[2]

P.G. Student, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, India[1]

Assistant Professor, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, India[2]

ABSTRACT: Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to re-authenticate their data even if a secret key of one single user has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

KEYWORDS: Authentication, Data Sharing, Cloud Computing, Forward Security, Backward Security

I.INTRODUCTION

The popularity and widespread use of "CLOUD" havebrought great convenience for data sharing and collection [2], [3], [4], [5], [6]. Not only can individuals acquire useful data more easily, sharing data withothers can provide a number of benefits to our societyas well.As a representative example,consumers in Smart Grid can obtain their energyusage data in a fine-grained manner and are encouragedto share their personal energy usage data with others,e.g., by uploading the data to a third party platform suchas Microsoft Hohm. From the collected dataa statistical report is created, and one can compare theirenergy consumption with others (e.g., from the sameblock). This ability to access, analyze, and respond tomuch more precise and detailed data from all levels ofthe electric grid is critical to efficient energy usage.Due to its openness, data sharing is always deployedin a hostile environment and vulnerable to a numberof security threats. Taking energy usage data sharingin Smart Grid as an example, there are several securitygoals a practical system must meet, including:

- **Data Authenticity**: In the situation of Smart Grid,the statistic energy usage data would be misleadingif it is forged by adversaries. While this issue alonecan be solved using well established cryptographictools (e.g., message authentication code or digitalsignatures), one may encounter additional difficulties when other issues are taken into account, suchas anonymity and efficiency;
- **Anonymity**: Energy usage data contains vast information of consumers, from which one can extractthe number of persons in the home, the types ofelectric utilities used in a specific time period, etc.Thus, it is critical to protect the anonymity of consumers in such applications, and any failures to doso may lead to the reluctance from the consumersto share data with others; and
- **Efficiency**: The number of users in a data sharingsystem could be HUGE (imagine a smart grid witha country size), and a practical system must reduce the computation and communication cost as muchas possible. Otherwise it would lead to a waste ofenergy, which contradicts the goal of Smart Grid.

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 6, June 2016

II.RELATED WORK

A. Identity-based Ring Trademark

Character based (ID-based) cryptosystem, presented by Shamir [4], disposed of the requirement for confirming the legitimacy of open key authentications, the administration of which is both time and cost expending. In an IDbased cryptosystem, the general population key of every client is effortlessly calculable from a string comparing to this current client's freely known personality (e.g., an email address, a private address, and so on.). A private key generator (PKG) then registers private keys from its expert mystery for clients. This property stays away from the need of declarations (which are essential in conventional open key base) and partners a certain open key (client personality) to each client inside of the framework. With a specific end goal to confirm an ID-based signature, unique in relation to the conventional open key based signature, one does not have to confirm the declaration first. The disposal of the declaration approval makes the entire check prepare more effective, which will lead to a critical recovery in correspondence and calculation at the point when countless are included (say, vitality utilization information partaking in shrewd framework).Ring mark is a gathering focused mark with security assurance on mark maker. A client can sign namelessly for a gathering all alone decision, while bunch individuals can be absolutely ignorant of being recruited in the gathering. Any verifier can be persuaded that a message has been marked by one of the individuals in this gathering (additionally called the Rings), yet the real personality of the underwriter is covered up. Ring marks could be utilized for shriek blowing,mysterious enrollment verification for impromptu gatherings [7] and numerous different applications which don't need confounded bunch development arrange yet require underwriter obscurity.

B. Forward-Secure Electronic digital Trademark System

Advanced mark plan in which general society key is adjusted however the mystery marking key is redesigned at standard interims to give forward security property: trade off of the present mystery key does not empower a foe to manufacture marks relating to the past. This can be utilizable to relieve the harm brought about by key introduction without requiring dissemination of keys. The development utilizes originations from the mark plots, and is ended up being forward secure predicated on the hardness of calculating, in the self-assertive prophet model. The development is furthermore very proficient.Past mark stay secure regardless of the possibility that uncover the present mystery key.

C. Security and Privacy-Enhancing Multicloud Architectures

Safety problems remain among the most astronomically tremendous road blocks when contemplating your adopting involving foriegn hotels. This kind of brought on various investigation pursuits, causing a volume of plans focusing on your sundry foriegn stability dangers. This understanding of getting by using a number of confuses has become distinguishing these system habits: Replication involving software sanctions to take delivery of a number of effects from one operation done within distinctive confuses also to compare all of them in the personal philosophy. This gives your utilizer to have data within the integrity from the outcome. Partition involving program Process in to tiers sanctions disuniting your common sense through the info. Thus giving adscititious aegis versus info seapage because of imperfections in the program common sense. Partition involving program common sense in to fragments sanctions disbursing the application form common sense to help distinctive confuses. This has a pair of positive aspects. Initial simply no foriegn company finds out your consummate program common sense. Subsequent, simply no foriegn company finds out the complete determined reaction to the application form. Hence, this kind of causes info in addition to program discretion. Partition involving program info in to fragments sanctions disbursing fine-grained fragments from the info to help distinctive confuses. The essential actual understanding is usually to utilize a number of distinctive confuses while doing so to help abate your jeopardies involving maleficent info adjustment, disclosure, in addition to practice tampering. Simply by adding distinctive confuses, your rely on postulation might be reduced to some postulation involving non-collaborating foriegn accommodation vendors. Further, this kind of establishing helps it be significantly more difficult on an outside assailant to help get back or perhaps tamper published info or perhaps software of your cement foriegn utilizer. These kind of strategies are managing on distinct foriegn accommodation levels, are in part blend having cryptographic methods, in addition to focusing on distinct employment scenarios.
- Data sharing within multi-cloud setting.

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 6, June 2016

- Data stability within multi-cloud.

III.PROBLEM STATEMENT

Backward Security is Provided to forward Secure identity based ring signature to increase Security level of identity based ring signature.To decrease key size, storage and transmission requirements Elliptic curve cryptography is used.

IV.PROPOSED SYSTEM

Proposed System provide backward security to forward Secure Identity based Ring Signature. In Previous System they focus on forward security but they are unable to provide backward security.Due to this Problem Backward Security is Provided.In this even if we revoke any person in ring, they are able to access the existing files. So that to overcome this our new system provide restrictions on users which we revoke to access the existing files.Ex.If there are ten users in ring and we provide forward security to all the members of ring.After that we decide to revoke two users of ring. For that we have to remove forward security constraints of these two users and provide restrictions on these two users for accessing existing files.For implementing this our proposed system will uses background security.Quality of Security in Our system is enhances while sharing of data on cloud.

V.SYSTEM ARCHITECTURE

The System Architecture acts as a workflow shown in figure.1 below. At first user register into the Private Key Generator system using user id and password and sign the file and after signing the file user upload that file onto cloud storage. The private key generator generate a public key and secret key based on identity of user and perform key updation.After this all other ring users download that files from cloud according to their public and secret keys.
Forward security is provided to this identity based ring signature. Due to this if secret key of signer is compromised by attacker then also all past signatures of that signer remain valid and secure. This architecture also provide backward security to identity based ring signatures.

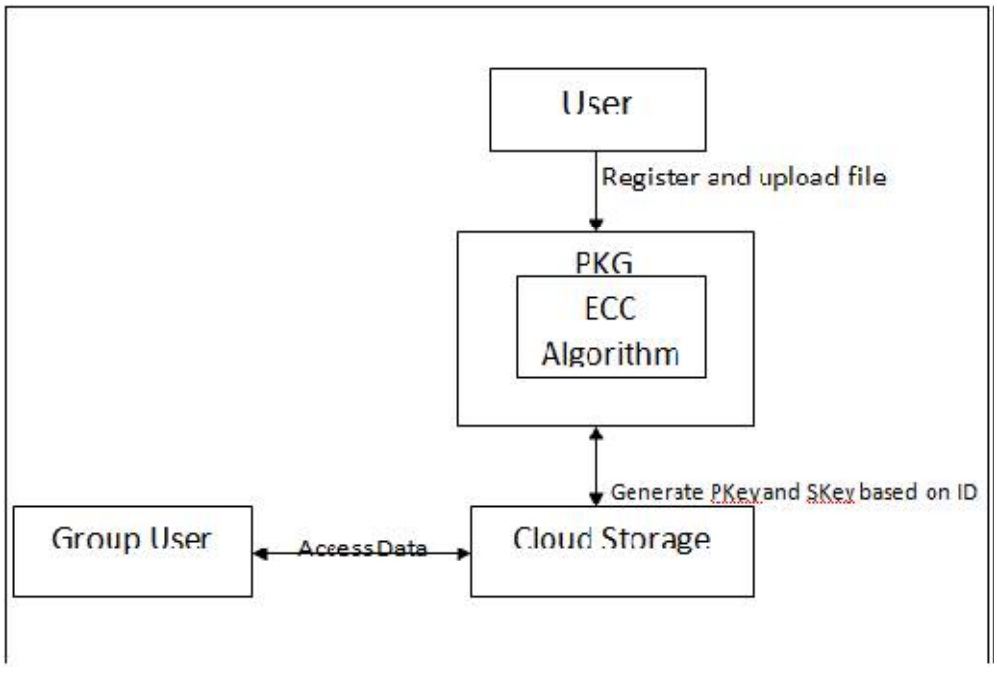

Figure1.Architecture of Proposed System

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 6, June 2016

The flow of Our System is as follows:
Owner Module: In this module the owner upload the doc to the System.
Registration Module: In this Module user register into System.
Authentication: In this module user authenticate into System.
Generate Secret Key (for each user): In this module the system will generate Secret key for each user.
Signing Doc for Sharing: In this module the user who wants to share a doc (selected users) he has to sign this data by using ID-based Signature.
Verify: In this module we list out all the data to login user. Then to access particular data he has to give his ID input parameter then based on the doc information and User information we calculate the signature for that particular doc and then we check the signature of that doc and the generated signature is same then that doc is accessible to that user.
Data Retrieval: Once the signature is verified by the system for a doc to which user is going to accesses? Then that doc is available for download.

VI. CONCLUSION AND FUTURE WORK

We Provide Backward Security to Forward Secure Identity Based Ring Signature in random Oracle Model using Elliptical curve Cryptography Algorithm. It is first in the literature to have this feature for forward secure identity based ring signature. Quality of Security of our system is increases due to the backward security. This system Provide authentic and secure data sharing in cloud computing. This system is very useful in applications where a number of users are used in sharing of data on cloud such as e-commerce, smart grid and ad-hoc network.We consider a provably secure scheme with the same features in the standard model as an open problem and our future research work.

REFERENCES

1. X.Huang,J.K.Liu,S.Tang,Y.Xiang,K.Liang,L.Xu and J.Zhou, "Cost Effective Authentic and Anonymous Data Sharing with Forward Security",IEEE Transactions,Volume 64, No: 6, 2015.
2. S. Sundareswaran, A. C. Squicciarini, and D. Li ,"Ensuring distributed accountability for data sharing in the cloud." ,IEEE Trans. Dependable Sec. Comput., 9(4):556–568, 2012.
3. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou. "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption", IEEE Trans. Parallel Distrib. Syst.,24(1):131–143, 2013.
4. X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud.", IEEE Trans. Parallel Distrib. Syst., 24(6):1182–1191, 2013.
5. Y. Wu, Z. Wei, and R. H. Deng., "Attribute-based access to scalable media in cloud-assisted content sharing networks",IEEE Transactions on Multimedia, 15(4):778–788, 2013.
6. 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.
7. E. Bresson, J. Stern, and M. Szydlo. " Threshold ring signatures and applications to ad-hoc groups.", In M. Yung, editor,CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, pages 465–480.Springer, 2002.
8. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. " Privacy- preserving public auditing for secure cloud storage.", IEEE Tans Computers, 62(2):362– 375, 2013.
9. G. Yan, D. Wen, S. Olariu, and M. Weigle., "Security challenges in vehicular cloud computing.", IEEE Trans, Intelligent Transportation Systems, 14(1):284– 294, 2013.
10. J. K. Liu and D. S. Wong, "Solutions to key exposure problem in ring signature" ,I. J. Netw. Secur., vol. 6, no. 2, pp. 170–180, 2008.
11. J. K. Liu, T. H. Yuen, and J. Zhou, "Forward secure ring signature without random oracles", in Proc. 13th Int. Conf. Inform. Commun. Security, vol. 7043, pp. 1–14,2011.
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, vol. 6402, pp. 166–183, 2012.
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.

BIOGRAPHY

Pritee A.Raut recieved the BE degree in computer engineering from Savitribai Phule Pune University in 2013,now pursuing ME in computer engineering from Vishwabharati Academy's College of Engineering,Savitribai Phule Pune University,Ahmednagar,Maharashtra, India in 2015-16.