International Journal of Engineering Research
Volume No.6, Issue No.12, pp : 544-548
ISSN:2319-6890 (online),2347-5013(print)
1 Dec. 2017

Secure Data Sharing over Cloud using Signatures

Harishchandra A. Akarte, Amrita A.Deorukkar
Department of Computer Engineering, Dr. Babasaheb Ambedkar Technological University
Corresponding Email: akarteharish@gmail.com

Abstract: Cloud data sharing have better ability to accessing data from anywhere to its end user. Sharing of secure data is more complicated with the progressive cloud computing. And exact analysis of shared data provides expansive benefit in society. Document sharing with huge no of users gives numerous issues like efficiency, access control, secrecy, data confidentiality. Ring signature is capable contender for accurate and authenticate analysis of data sharing system. We additionally provide bi-linear based ring signature schemas with forward security. we calculate sign for each document then make group sign for particular no of users. Splitted that sign with individual users and once currently generated sign is verified for document then document is ready to accessible for users. If any condition secret key of any single user has been bargained, then exact and all earlier generated signature remains valid. This property is particularly work on critical and large scale data sharing system.

Keywords: Authenticate, Contender, Cloud computing, Security, Signature

Introduction

Cloud computing has been generating the lot interest, lot competition and lot of enthusiasm in our computing industry. It can allow us to create, customize and configure the applications online. Not only the people will acquire helpful knowledge but also sharing data with others will give variety of advantages to the public and individuals [1].

Data sharing and its benefits include good customer support and better understanding of the needs of the customer and Shared data can be used to improve the modeling, analysis and risk tools [2]. The ring signature is promising applicant to develop a mysterious and authentic data sharing system. It allows a data owner to anonymously confirm his information which can be put into the cloud for storage or analysis reason. Data sharing is always deployed in number of security threats.

We considering consumer in a smart grid they acquire their energy practice data would be misleading. They have vast information of consumers; one can evaluate their energy consumption with others. This ability to access, analyze, and share data from all stages of the electric grid is dangerous to well-organized energy usage. Due to extensive use of cloud we contend that, it will be difficult to provide good solution for securing the data at present. Therefore, our goal is to make increment enhancements for securing data in cloud [1]. The design of bi linear based ring Signature is a promising

contender to develop a mysterious and authentic data sharing system. In this paper, the upgraded concept of the secure bi linear based signature provides so as to have a ring signature forward security. The bi linear based ring signature, an efficient solution on applications requiring data authenticity and anonymity. This property is especially important to big scale data sharing system, as it is impossible to ask all data owners to re-authenticate their data even if a secret key of any user has been comprised.

Fig.1. shows that,as example of smart grid, by uploading the data to the third party plat-form which is shown in (Fig.1). From the collected data a statistical result is created. One can Compare their energy usage with others. This ability to access, manage, and share to much more accurate and precise data from every stages of the electric grid is difficult to well-managed energy usage.

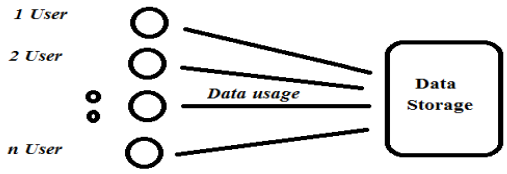


Fig.1. Energy usage in smart grid

A variety of participants focus to this technology, due to the services reduces their computation cost and reliable data transmission in a well-organizedmanner. there are plenty of security goals in a piratical must meet as well as,

1. Secrecy: The amount of data sharing system would be vast. There are many social networking sites with millions of users communicating with each other, Therefore, it is difficult to protect secrecy of customers in such requests.

2. Data genuinity: If we consider situation of smart grid the energy usage of data might be fake and ambiguous, so it is dangerous to maintain and update genuine data. It would lead to a waste of energy, which contradicts the goal of security.

3.Data confidentiality: The Cloud provider usually has direct access for data and hence is more likely to steal data for illegal purposes. Unauthorized users not only cable to access data but also share information at any given time.

4. Data availability: There are other security issues in data sharing system which are equally important, such as

ISSN:2319-6890 (online),2347-5013(print)
1 Dec. 2017

availability (service is provided at an acceptable level even under network attacks.

In this paper we investigated fundamental securitytools for realizing these four properties we described.There are other security issues in a data sharingsystem which are equally important, such as data availability (service is provided at an acceptable level even under network attacks), Data Integrity, Data Segregation and access control (only eligible userscan have the access to the data). But the study of those issues is out of the scope of this paper [2,3,4,5,6,7,8,9,10].

II. Related Work

There is some existing system which are followed.

A. Practical and Provably Secure Coalition-Resistant Group Signature Scheme [12]

This paper address the new provably secure group signature and a companion identity escrow scheme that are significantly more efficient. The security, this scheme allows a group member to sign messages anonymously on behalf of the group.

In its interactive, identity escrow form, this scheme is proven secure and coalition-resistant under the strong RSA and the decisional Diffie-Hellman assumption. The security of the interactive variant. therefore, group signature scheme, relies additionally on the Fiat-Shamir heuristic (also known as the random oracle model). In opposite to ordinary signatures they provide a secrecy to the signer that a verifier can only tell that a member of some group signed. Therefore, any group signature can be “opened" by a designated group manager so they reveal unambiguously the identity of the signature's originator.

B.Privacy-Preserving Public Auditing for Secure Cloud Storage [11]

They propose a privacy-conserving public analyzing system for data storage safety in cloud computing. which is based on homomorphic-linear authenticator and random masking to guarantee. They eliminate the burden of cloud user from the tedious and expensive analyzing task, along with ease the users fear of their redistributed data crack. TPA can concurrently manage the numerous analyzer term from various users for outsourced data logs and later expand the privacy-conserving public analyzing protocol into a multiple user setting, where the they can perform multiple auditing tasks in a batch manner for better efficiency. but they don’t have guarantee about multiple auditing task as compared to single auditing task.

C.New Efficient Threshold Ring Signature Scheme Based on Coding Theory [14]

Ring signature is a good identification technique, where a signer can anonymously authenticate a message depends on coding theory. Total system depends on coding theory. In this paper they have presented a new threshold ring signature scheme based on coding theory. This protocol is a very simple generalization of the Stern identification scheme. They observe that the notion of weight of vector particularly went well in the context of ring signature so the approach of ad hoc set coincide well to the approach of accurate sum of generator matrices and is adaptable with the approach of sum of vectors of less weight. So the protocol is the non-generic protocol based on coding theory (as usual for code based protocol). And it is very fast compared to other number theory based protocols.

D. Anonymous Identification in Ad Hoc Groups

They introduced Ad Hoc Anonymous Identification schemes. The Techniques are based on the accumulator with one-way domain. And natural expansion of cryptographic accumulators is brought in this concept. This specific efficient implementation based on the Strong RSA Assumption. They Used the Fiat-Shamir transform and obtain constant-size, signer-ambiguous group and ring signatures. Their main system in the construction of AdHoc Anonymous recognition schemes is a new cryptographic primitive, accumulator with one-way domain, which expands the approach of a collision-resistant accumulator.

E. Solutions to Key Exposure Problem in Ring Signature

They propose key-insulated ring signature scheme. They can allow any adversary to build a valid key-insulated ring signature for the particular time periods. So they suggest solutions to the key exposure problem in ring signature. Also the size of the signature in scheme grows linear with the number of users. It is an interesting open problem to construct a key-insulated ring signature scheme with a constant size to the number of users. Both of them allow a (t,n) threshold setting. The System is based on security in the random oracle model.

III. Proposed Work

A.Bi linear based ring signature:

Recently the bi linear pairing has been found advantageous in designing various cryptographic schemas especially for those using id based public keys. It is still important to design new schemes that require less pairing operation to achieve better performance. In bi linear based ring signature public key of any single user has been easily accessible, from a string corresponding to this user’s publicly known identity. A private key generator calculates their private key from its master secret key [3].

They avoid the validity of certificates first and it makes the whole verification process more flexible, which will lead significant in communication and computation when a huge number of users are involved.

Ring signature were invented by Ron Rivest, Adi Shamir and YealTauman and introduced at ASIACRYPT. Ring signature is type of digital signature with privacy protection on signature producer. It can allow user to construct a secure and valid data sharing system. By using This method owner can anonymously authenticate his document which can be put into the storage at different places.

As shown in fig 2. the overall and main theme of system as the Admin and group members. Admin upload the file into the cloud group member retrieved the file from cloud. before that

ISSN:2319-6890 (online),2347-5013(print)
1 Dec. 2017

assign id with particular members or users. Using this id generate sign with particular no of users. And splitted that sign to the all individual users. A verifier can be convinced that a message signed by one of the members in the group but the actual identity of the signer is hidden. After successful verification of signature document or data available for users. Ring signature is type of group-oriented signature with the privacy protection.

The Ring signature is used for anonymous membership authentication for ad-hoc groups and more other applications which do not want complicated group formation stage but require signer anonymity.

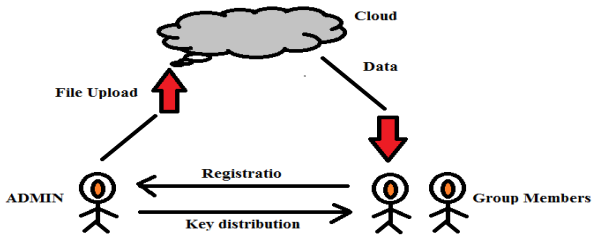


Fig. 2. Basic architecture

Many of the users are a getting attracted to this technology due to the services involved in it the followed by the reduced computation followed by the cost and also the reliable transfer of data is performed in the system very effectively.

B. Motivation

The bi linear based ring provides the great anonymity, accuracy and availability. It provides correct solution on data sharing over the huge no of participants.

To get higher level of security, it can add more user in a ring. Key exposure is a basic drawback of digital signature. If the private key of a signer has been compromised, all generated signatures are worthless. Once the key leakage is recognized, then key revocation must be raised in order to prevent the generation of any signature using the compromised secret key [3,4,5,6].

C. Contribution

In this paper we proposed new idea called forward secure bi linear based ring signature which is fundamental tool for building reliable, unspecified data sharing. Initially we offer the proper definition of forward secure bi linear based ring signature. we make appropriate plan for forward secure bi linear based ring signature. No previous bi linear based ring signature schemas in literature have the property of forward security, and we are the first to provide this feature;

1 We prove the security of the proposed scheme in the random oracle model, under the standard cryptographic assumptions.

2 We successfully compared h-mac (hash based message authentication code) and id based ring signature schemas.

Our practical implementation is in the following way:

1. Identity basic settings, they generate sign for each users depending on their unique id parameter. Then generate sign for group signature.
2. Append that sign with calculated signature and group signature.
3. The size of secret key is just an integer.
4. We do not need any pairing in any phase.

Our design of system simultaneously accomplish security and performance support as follows.

D. Algorithm

Step 1: Initialize the public identity of each participant. this stage only defines public information of groupmembers;such as houses address.

Step 2: data owner uploads his own data depending on that generate sign for each user, then make group sign for particular no of user. also appends calculated sign and group signature.

Step 3: by verifying the ring signature, they pass token from any one of the member, ifone canhave guaranteed that data is given by valid resident from the ring members. therefore, data verification efficient and secrecy of data retrieval maintain and does not required validity of certificates

IV. ModuleDescription

After meticulously analyzing, the system has been described to have the following modules:

1. Owner:

In this module the owner transfers the doc to the System.

2. Registration:

In this Module user register into System.

3. Authentication:

In this module user validate into System.

4. Generate Secret Key (for each user):

In this module the system will produce Secret key for every user.

5. 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 block ring Signature. (For selected users)

6. Verify (background processing):

In this module, we classify out all the data to login user. Then to access specific data one has to give his identification input parameter and based on the doc information and User information, the signature is calculated for that particular doc and then we cross check the signature of that doc and if the obtained signature is same then that doc is permitted to access by that user.

7. Data Retrieval: Once the signature is verified by the system for a doc to which user is going to access, then that doc is available for download.

8. Analysis: Comparative analysis between existing (HMAC) based and bi linear based block ring signature will have done on basis of execution time parameter.

ISSN:2319-6890 (online),2347-5013(print)
1 Dec. 2017

V. Flow Diagram

Fig. 3. shows overall design of secure data sharing over cloud. These Various modules described in detail in module description.

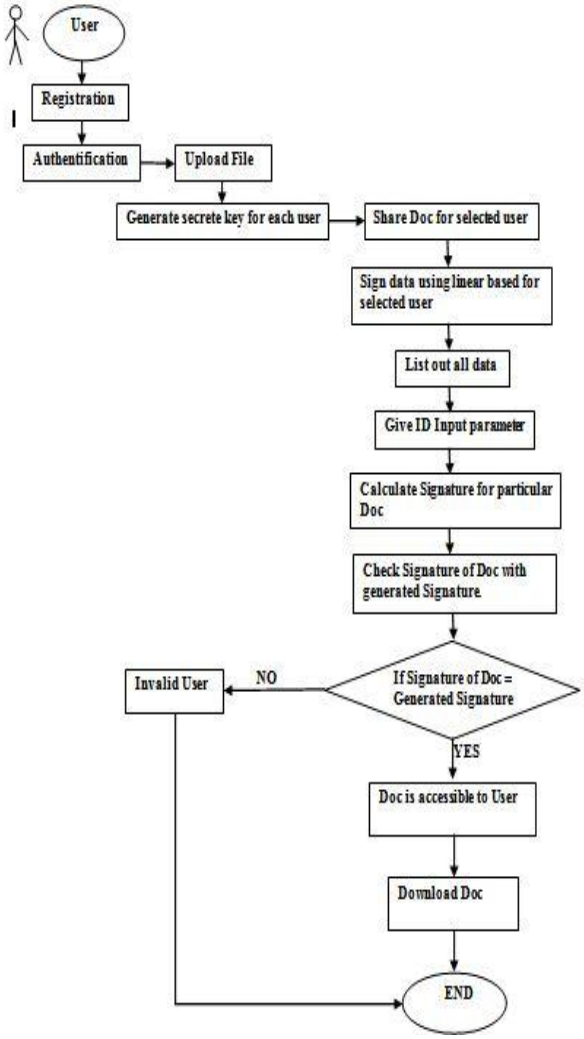


Fig. 3.Flow diagram

VI. Work flow

This section is delivered to the description and analysis of proposed bi- linear based ring signature schemas.

Notations:

1 S, p -two random k-bit prime numbers.
2 H1, H2 - Two hash functions
3 (S,p)-master secret key msk
4 r- fixed parameter.
5 e- choose random prime no

Setup: Consider the identities and secret key of user valid only in T period and make time interval as public. And set the message space M= {0,1}*, users key space D, signature space & .H1 :{ 0, 1}*→ Z*N and H2 :{ 0, 1}*→ {0, 1}.Consider a security parameter lymbda. The public parameters are (k,r,e,H1,H2) and msk is (s,p). and s= 2s'+1, p=2p'+1

Extract: Any user i, list of system parameter identity IDi ε {0, 1}* requests for a secret key at time period T ,where 0 ≤t < T, msk be the master secret key, consider that identity IDi corresponds to user secret key (ski,0) (IDi, ski,0) is an input-output pair of Extract with respect to parameter and msk.

Update: on uses secret key ski, t for the time period t, they updates the outputs of users secret key ski,t+1, for the time period t+1

Sign: to sign a message m and m ε {0, 1}* in time period t, identities of the members L = {ID1,....,ID n}, outputs of the signature for the list of identities L in time period t .generate group sign for each user

Split:for each user divide sign separately from ring signature m= a+r

a=a1+a2+a3+…an, r= r1+r2+r3+…rn.

Append:join easily with calculated sign and group sign as per the no of users

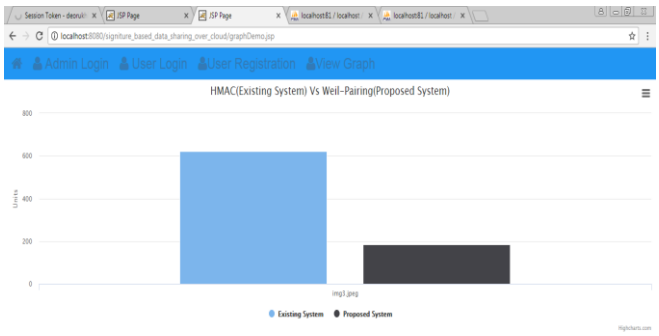
m= a1+r1

Verify: To verify a signature $ for a message m, and no of identities L and the time period t, set L = {IDi belongs (0,1)},* {i belongs(1,0)}

m belongs M, &belongs $, checks outputs either valid or invalid.

VII. Comparisonand Result

We compare our scheme with h mac and id based using bi linear based ring signature scheme in terms of features, computation and time as shown in figure below, note that the verification for non bi linear based ring signature scheme requires validity of certificates first. Therefore, we exclude cost, time and space for those number of participants.



VIII.Conclusion

Inspired by realistic challenges in data sharing we proposed new bi linear based ring signature schemas with forward security. because of this well-organized idea our system provides unconditional secrecy and anonymity. our system generate sign for particular user depending on their id input parameter. combine sign for all selected users after that distributed sign with each users once generated sign is match with previous signatures then documents areavailable, this system is more efficient and its does not required any paring

ISSN:2319-6890 (online),2347-5013(print)
1 Dec. 2017

mechanism. our project is used in many practical applications specially for those participants who required authentication and privacy like e-commerce activity.

References

i. *"Security Issues for Cloud Computing ". Technical Report utdcs-02-10,Department of Computer Science University of texas at Dallas.feb 2010. Kevin Hamlen, The University of Texas at Dallas, USA,MuratKantarcioglu, The University of Texas at Dallas, USA, Latifur Khan, BhavaniThuraisingham.*

ii. *"Secure Data Sharing in Cloud", DananThilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo.*

iii. *"Cost Effective and anonymous data sharing with forward security ". Xinyi Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member, IEEE transactions on computers, vol. 64, no. 2016*

iv. *"Cost-Effective Authentic and Anonymous Data Sharing with Forward Security", Praveen Kumar, P.Suman Prakash, Dr.S.Prem Kumar, Volume 2, Issue 12, December-2015, pp. 1126-1131.*

v. *"Profitable Authentic and Anonymous Data Sharing with Advance Security",priyanka, N. somanna, ISSN 2321-8665 Vol.04, Issue.12, September-2016, Pages:2221-2224*

vi. *"cost Effective Authentic and Anonymous DataSharing with Forward Security".Shreyas S. Barde, Rupa R. Kandule, Laxmi R. Salunke, Prof. Ashok Kumar.Department of Computer Engineering, G.S. Moze College of Engineering, Balewadi, Pune, MH, India, vol4, January 2016.*

vii. *"Survey on Forward Security for Authentic and Anonymous Data Sharing with Auditing Integrity".Vidya A. Gaikwad, sachin D. Babar, PhD International Conference on Internet of Things, Next Generation Networks and Cloud Computing.*

viii. *"User Privacy and Security in Cloud Computing" , AL-Museelem Waleed, a, Li Chunlin, International Journal of Security, Vol. 10, No. 2 (2016), pp.341-352.*

ix. *"Cloud Computing: Security Issues and Research Challenges", Rabi Prasad Padhy, ManasRanjanPatra, Suresh Chandra Satapathy, Vol. 1, No. 2, December 2011.*

x. *"Security Issues and their Solution in Cloud Computing." Prince Jain,International Journal of Computing & Business Research ISSN (Online): 2229-6166.*

xi. *" Privacy-Preserving Public Auditing for Secure Cloud Storage". Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian-Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE.*

xii. *Giuseppe AtenieseJanCamenischMarcJoyeGeneTsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme". Annual International Cryptology Conference, 2000.*

xiii. *" Ensuring Distributed Accountability for Data Sharing in the Cloud",Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin.*

xiv. *Carlos Aguilar Melchor, Pierre-Louis Cayrel, Philippe Gaborit, and Fabien Laguillaumie "New Efficient Threshold Ring Signature Scheme Based on Coding Theory", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 57, NO. 7, JULY 2011*

xv. *M. Abe, M. Ohkubo," 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.*

xvi. *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.*

xvii. *M. H. Au, J. K. Liu, T. H. Yuen, "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.*

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

xix. *M. Bellare 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 Sci.*

xx. *M. Bellare and S. Miner. A forward-secure digital signature scheme. In Crypto'99, volume 1666 of Lecture Notes in Computer Science.*

xxi. *J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau. "Security and privacy-enhancing multicloud architectures". IEEE Trans. Dependable Sec. Computer.*

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

xxiii. *A. Boldyreva. "Efficient Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap Diffie-Hellman Group Signature"*