International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Forward Security Authentication on Data Sharing Cloud Computing

M RAVI KUMAR [1]& SHILPA REDDY BALUPALLE[2]

[1] ASSOCIATE PROFESSOR Dept. of CSE SVR ENGINEERING COLLEGE, AYYALURU, NANDYAL Email: - ravi2kinus@gmail.com

[2]PG-Scholar Dept. of CSE SVR ENGINEERING COLLEGE, AYYALURU, NANDYAL Email: - shilpa.balupalle@gmail.com

Abstract

Cloud Computing is ceaseless growing latest technology in IT industry, academia and business. The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing is highly accessible, flexible technology that puts hardware, software, and virtualized resources. Cloud computing infrastructure works over the internet on demand basis. Main features of cloud computing is that on-demand capabilities, broad network access, resource pooling, rapid elasticity ,measured service scalability and provides shared services to user on demand basis in distributed environment. Commonly available cloud computing service providers are Google, Yahoo, Microsoft, Amazon etc. The details of cloud services are abstracted from users. The most common issues of cloud computing as efficiency, integrity and authenticity. Moreover, users are unaware of location where machines which actually process and host their data. The motivation of this paper is to propose a secure data accessing and sharing scheme, for public clouds.

Keywords: Authentication, Data Sharing, Cloud Computing, Forward Security

1. INTRODUCTION

Forward secure identity based ring signature for data sharing in the cloud provide secure data sharing within the group in an efficient manner. It also provide the authenticity and anonymity of the users. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to secretly authenticate his data which can be put into the cloud for storage or analysis purpose. The system can be avoid costly certificate verification in the traditional public key infrastructure setting becomes a bottleneck

for this solution to be scalable. Identity-based ring signature which eliminates the process of certificate

Verification can be used instead. The security of ID-based ring signature by providing forward security: If a secret key of any user has been rev, all previous generated signatures that include this user still remain valid. The 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 conceded. Accountability and privacy issues regarding cloud are becoming a significant barrier to the wide adoption of cloud services. There is a lot of advancement takes place in the system with respect to the internet as a major concern in its implementation in a well effective manner respectively and also provide the system in multi-cloud environment. Many of the users are getting attracted to this technology due to the services involved in it followed by the reduced computation followed by the cost and also the reliable data transmission takes place in the system in a well effective manner respectively.

System Architecture:

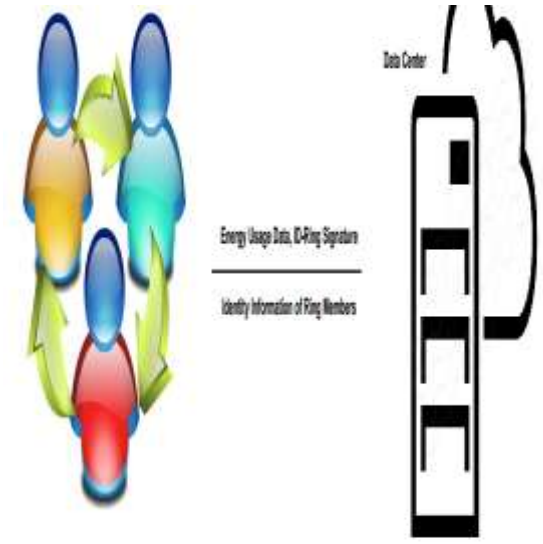

Fig: - 1 A Solution based on ID-based Ring Signature

2. RELATED WORK

Existing system:

Identity-based (ID-based) cryptosystem, introduced by Shamir, eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming.

Data Authenticity: In the situation of smart grid, the statistic energy usage data would be misleading if it is forged by adversaries. While this issue alone can be solved using well established cryptographic tools (e.g., message authentication code or digital signatures), one may encounter additional difficulties when other issues are taken into account, such as anonymity and efficiency.

Anonymity: Energy usage data contains vast information of consumers, from which one can extract the number of persons in the home, the types of electric 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 do so may lead to the reluctance from the consumers to share data with others.

Proposed system

In this paper, we propose a new notion called forward secure ID-based ring signature, which is an essential tool for building cost-effective authentic and anonymous data sharing system. For the first time, we provide formal definitions on forward secure ID-based ring signatures. Ring signature is a group-oriented signature with privacy protection on signature producer. A user can sign anonymously on behalf of a group on his own choice, while group members can be totally unaware of being conscripted in the group. Any verifier can be convinced that a message has been signed by one of the members in this group (also called the Rings), but the actual identity of the signer is hidden. In an ID-based cryptosystem, the public key of each user is easily computable from a string corresponding to this user's publicly known identity (e.g., an email address, a residential address, etc.). A private key generator (PKG) then computes private keys from its master secret for users. In order to verify an ID-based signature, different from the traditional public key based signature, one does not need to verify the certificate first. The elimination of the certificate validation makes the whole verification process more efficient, which will lead to a significant save in communication and computation when a large number of users are involved (say, energy usage data sharing in smart-grid).

3. IMPLEMENTATION

Data Authenticity:

In a cryptographic sense, authenticity indicates that a message was endorsed by a particular principal. This principal may endorse multiple messages, and the same authentication tag can validate distinct messages. In a data flow sense, authenticity guarantees the provenance of a message, but it does not distinguish between different messages from the same principal. A mere Authenticity check does not protect against replay attacks: a message that was authentic in a previous run of the protocol is still authentic

Anonymity:

Anonymous communication allows users to send messages to each other without revealing their identity. It is aimed at hiding who performs some action, whereas full privacy requires additionally hiding what actions are being performed. In the context of distributed computation, anonymity allows hiding which users hold which local inputs, whereas privacy requires hiding all information about the inputs except what follows from the outputs.

Efficiency:

The number of users in a data sharing system could be huge and a practical system must reduce the computation and communication cost as much as possible securing transactions online transactions typically require: message integrity to ensure messages are unaltered during transit message confidentiality to ensure message content remain secret non-repudiation to ensure that the sending party cannot deny sending the received message and sender authentication to prove sender identity

Sign: On input a list param of system parameters, a time period t, a group size n of length polynomial in λ, a set $L = \{IDi \in \{0, 1\}^* / i \in [1, n]\}$ of n user identities, a message $m \in M$, and a secret key $sk_{\pi,t} \in D$, $\pi \in [1, n]$ for time period t, the algorithm outputs a signature $\sigma \in \Psi$.

Verify: On input a list param of system parameters,a time period t, a group size n of length polynomial in λ, a set $L = \{IDi \in \{0, 1\}^* / i \in [1, n]\}$ of n user identities, a message $m \in M$, a signature $\sigma \in \Psi$, it outputs either valid or invalid.

Update: On input a user secret key $sk_{i,t}$ for a time period t, the algorithm outputs a new user secret key $sk_{i,t+1}$ for the time period $t + 1$.

Experimental Results

Fig:-2 Group user Creation

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

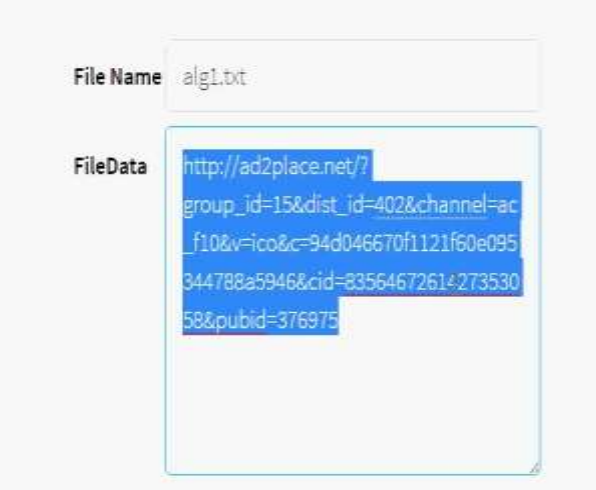

Fig:-3 File Data

Fig:-4 Key generation

Fig:-4 Signature Data

4. CONCLUSION

Forward Secure ID-Based Ring Signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-based setting. Our scheme provides unconditional anonymity and can be proven forward-secure unforgeable in the random oracle model, assuming RSA problem is hard. Our scheme is very efficient and does not require any pairing operations. The size of user secret key is just one integer, while the key update process only requires an exponentiation. We believe our scheme will be very useful in many other practical applications, especially to those require user privacy and authentication, such as ad-hoc network, ecommerce activities and smart grid. Our current scheme relies on the random oracle assumption to prove its security. To improve security for authentication on ring members using MAC algorithm. SHA-1 and MD5 algorithm is used for data encryption. In this algorithm is used for large size of data should be encrypted. Sharing data on one ring members to another ring members. Then enhance security on data sharing and upload the data on cloud. 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] 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] 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 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] A. 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.