International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184, Volume 5, Number 1 (February 2016), pp.27-32

http://www.meacse.org/ijcar

Dynamic and Flexible Group Key Generation Based on User Behaviour Monitoring

R.Shanmuga Sundaram, D.Arthy and T.Priya Radhika Devi

Department of Computer Science and Engineering, Mailam Engineering College, Mailam, India

Abstract

In cloud computing data owner updates the information to the remote cloud server for data access. data owner appoints members for data utility and data updation. Members have to get permission for the data updations from the data owner. Members will have their user name, key, group key for access. If existing member is revoke from that group, group key is automatically changed and updated to all the members of that group. the modification is group key can be changed in case of new member is added in that group or existing member is resigned by themselves from the group or data owner terminates the member or cloud terminates the member in case of misbehavior (DDOS Attack, same data download), updated new key is sent to the corresponding users through E-mail.

Keywords – Diffie-Hellman methodology, Public auditing, shared data, User revocation.

Introduction

In today's Computing world Cloud computing is one of the largest innovations that uses advanced computational power and it improves information sharing and information storing
Capabilities, this has improved storing capability on comparing with others. Main problem in cloud computing was issues of information integrity, information privacy and information access by unauthorized users. The verification can be done by TPA (Trusted Third Party) or user from the group in cloud. Trusted Third Party is the outside party who
will effectively check data was correct. TTA also employed to store and share information in cloud computing. Modification and sharing of information is kind of straightforward as a gaggle. To verify integrity of the shared information, members within the cluster must calculate signatures on all shared information blocks. Completely different blocks in shared information area unite usually signed by completely different users owing to information modifications performed by completely different users. User revocation is one of the largest security threats in information sharing in teams. During user revocation shared information block signed by revoked user must transfer and re-sign by existing user. This task is very inefficacious owing to the big size of shared information blocks on cloud. PANDA and is that the new public auditing mechanism for the maintaining integrity of shared information with economical user revocation within the cloud. This mechanism relies on proxy re signatures concept that permits the cloud to re-sign blocks on behalf of existing users throughout user revocation, so that downloading of shared information blocks isn't needed. PANDA Plus is that the public auditor that audits the integrity of shared data while not retrieving the complete information from the cloud. It also monitor batch to verify multiple auditing tasks simultaneously. Batch auditing done as number of process per second. The main characteristic that was taken into account is Correctness of data, Efficient and Secure User Revocation, Public Auditing, and Scalability. This study work comprises the ECC Algorithm, proxy re-signature, Batch Auditing process, and Comparative study.

LITERATURE REVIEW

1: Public Auditing for Shared Data with Efficient User Revocation in the Cloud

With data services in the cloud, users can easily modify and share data as a group. To ensure data integrity can be audited publicly, users need to compute signatures on all the blocks in shared data. Different blocks are signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks, which were previously signed by this revoked user must be re-signed by an existing user. The straight forward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a novel public auditing mechanism for integrity of shared data with efficient user revocation in mind by utilizing proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

2: Compact Proofs of Retrievability

In a proof-of-retrievability system, a data storage center must prove to a verifier that he is actually storing all of a client's data. The central challenge is to build systems that are both efficient and provably secure that is, it should be possible to extract the client's data from any prover that passes a verification check. In this paper, we give the first proof-of-retrievability schemes with full proofs of security against arbitrary adversaries in the strongest model, that of Juels and Kaliski. Our scheme built from BLS signatures and secure in the random oracle model, has the shortest query and response of any proof-of-retrievability with public verifiability. Our second scheme, which builds elegantly on pseudorandom functions (PRFs) and is secure in the standard model, has the shortest response of any proof-of-retrievability scheme with private verifiability (but a long query). Both schemes rely on homomorphic properties to aggregate a proof into one small authenticator value.

3: Ensuring Data Storage Security in Cloud Computing

Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

4: Provable Data Possession at Untrusted Stores

We introduce a model for provable data possession (PDP) that allows a client that has stored data at untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems. We present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our

implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation.

5: Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing

Cloud computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor, on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public verifiability or dynamic data operations, this paper achieves both.We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for seamless integration of these two salient features in our protocol design. In particular, to achieve efficient data dynamics, we improve the Proof of Retrievability model by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. Extensive security and performance analysis show that the proposed scheme is highly efficient and provably secure.

PROBLEM STATEMENT

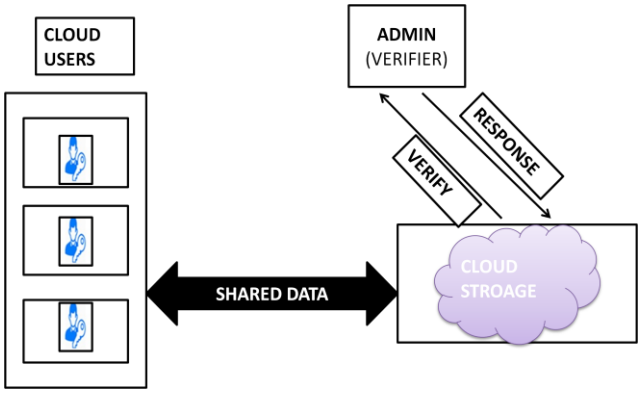
In an existing there are some of threats are available such as more time consuming to compute the re signature process and also it took more computation resources because of using provable data possession, proxy re-signature .so we implementing the dynamic key generation using Diffie-Hellman algorithm and ECC algorithm.

DESIGN OBJECTIVES

Our proposed mechanism should achieve the following properties: (1) Prove the Correctness: Trusted Party Auditor verifies the access of the owner to maintain the integrity of the data. (2) Secure User Revocation: when user resign from the cloud group the entire key of the group will be changed dynamically to provide the security. (3) Public Auditing: TPA auditing the common shared data to check any misbehavior of the users.(4) Scalability: the dynamic key generation is also implemented for the high scalability, the number of the auditing task can be done simultaneously by the public auditor

ARCHITECTURE

Group key can be changed in case of New member is added in that group also member can resign from the group by themselves or data

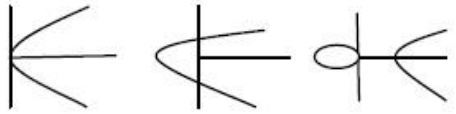


METHODOLOGIES

The methodology is used to measure and implement the Dynamic and secured key to the cloud group.

ECC Algorithm

The Elliptic Curve Cryptography have number of features such as Smaller Key size, higher speed, lower power consumption, Bandwidth savings, Storage efficiencies and smaller signatures.
The ECC Algorithm possess key with in shorter duration.
Ecc over Prime Fields,
$y2 = x3 + ax + b$
Ecc over Binary Fields,
$y2+xy = x3+ax2+b$
Where,
x, y - points on the curve,
a, b – coefficients



$y^2=x^3-1$ $y^2=x^3+1$ $y^2=x^3-x$

They may be applied at many areas as wireless communication devices, Smart cards, Web servers that need to handle many encryption sessions, any application where security is needed but lacks the power, storage and computational power that is necessary for our current cryptosystems.

Batch Auditing

Auditing is the process of checking whether the data file have all the information in it without missing or error. The broken data file happens due to untrusted user from cloud group. The processes under batching are user membership checking in group, random generation of key. Numbers of files are verified simultaneously by the users or third party auditor. Third party is the outside party who will effectively check the files are correct and not misused.

Comparative Study

Algorithm	E/D*	DS*	KX*
RSA	Yes	Yes	Yes
ECC	Yes	Yes	Yes
DSS	No	Yes	No
Diffie-Hellman	No	No	Yes

E/D* - Encryption/Decryption,

DS* - Digital Signature,

KX* - Key Exchange,

On comparing elliptic curve cryptography with the diffie-hellman algorithm, diffie-hellman algorithm have the process of key exchange and it can't be used for encryption, decryption, generation of digital signature. even though RSA algorithm have the property of all the three: encryption, decryption, digital signature, key exchange it has larger key size.

CONCLUSION

We proposed a new public auditing mechanism for provide integrity when user revoke from the cloud. The auditing mechanism involve in checking the user misbehavior actions. And also verify the data denial of service attacks. This will reduce the computational and communication cost and also the public Auditing is simpler when the key size is smaller.

It can save a significant amount of computation and communication resources during user revocation in the cloud.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912, 2013.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf.Computer and Comm. Security (CCS'07), pp. 598-610, 2007.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'08), pp. 90-107, 2008.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th ACM/IEEE Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[6] Q. Wang, C. Wang, J. Li, K. Ran, and W. Lou, "Enabling Public
Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[8] Y. Zhu, H. Wang, Z. Hu, G.-J.Ahn, H. Hu, and S.S. Yau, "Dynamic Audit Services for Integrity Verification of OutsourcedStorages in Clouds," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Jan. 2012.

[10] Y. Zhu, G.-J.Ahn, H. Hu, S.S. Yau, H.G. An, and C.-J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Trans. Services Computing, vol. 6, no. 2, pp. 227-238, Apr.-June 2013.

[11] "Practical Short Signature Batch Verification", A.L. Ferrara, M. Green, S. HohenbergerProc., Cryptographers'Track at the RSA Conf. Topics in Cryptology (CT-RSA'09), pp. 309-324,2009.

[12] "Proxy Resignatures: New Definitions, Algorithms and Applications", G. Ateniese and S. Hohenberger, Proc. 12th ACM Conf. Computer and Comm. Security (CCS'05), pp. 310-319, 2012.

[13] "Hourglass Schemes: How to Prove That Cloud Files are Encrypted", M. van Dijk, A. Juels, A. Oprea, R.L. Rivest, E.Stefanov,and.Triandopoulos, Proc. ACM Conf. Computer and Comm. Security (CCS'12), pp. 265-280, 2012.

[14] "Public Auditing for Shared Data withEfficient User Revocation in the Cloud", B. Wang, B. Li, and H. Li,Proc. IEEE INFOCOM,pp. 2904-2912,
2013.

[15] "How to Share a Secret", A. Shamir, Comm. ACM, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[16] "Storing Shared Dataon the Cloud via Security- Mediator", B. Wang, S.S.M. Chow, M. Li, and H. Li, Proc. IEEE 33rd Int'lConf. Distributed
Computing Systems (ICDCS'13), pp. 124- 133,July 2013.

[17] "Proxy Re-signatures: New Definitions, Algorithms and Applications", G. Ateniese and S. Hohenberger, Proc. 12th ACM Conf. Computerand Comm. Security (CCS'05), pp. 310-319, 2005.
[18] A. Shamir, "How to Share a Secret," Comm. ACM, vol. 22, no. 11,pp. 612-613, Nov. 1979.
[19] B. Wang, H. Li, and M. Li, "Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics," Proc. IEEE Int'l Conf. Comm. (ICC'13), pp. 1946-1950, June 2013.
[20] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS'13), pp. 124-133,July 2013.