IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DYNAMIC BIG DATA AUDIT ASSISTANT FROM UNAUTHORIZED ACCESS IN CLOUD COMPUTING STORAGE

[1] Dr.M.SRINIVASAN, [2]Mrs . B.KEERTHI, [3]S.ANUSHREE, [4]NOOR FOWZIYA, [5]K.PREETHI

B.TECH - INFORMATION TECHNOLOGY ,
P.S.V College Of Engineering And Technology
Krishnagiri,TamilNadu

Abstract:

Collusion between revoked users and cloud service providers can pose a threat to the security of cloud storage data. If the original legitimate users cannot be revoked securely, it will lead to the leakage of shared data, thus affecting the security of cloud storage. In this project, we combine vector commitment and anonymous revocation of group signature to propose an integrity audit scheme for cloud storage data that can support data medication. The anonymity of the group signature ensures that users' privacy information will not be snooped by the server. The proposed scheme supports the dynamic operation of stored data by legitimate group users besides data owners. When the user behaves improperly, the membership can be revoked by the group manager. After the user modified data is stored in the cloud, whether the cloud server correctly stores the data can be audited by a trusted third party. Security analysis and experimental results demonstrate that our scheme is secure and efficient.

Index Terms **- cloud computing, cloud storage, Data Integrity, security,Auditing**.

Introduction:

With the development and improvement of cloud computing technology, many individuals and enterprises outsource data to cloud service provider (CSP) for datacomputing and data storage. While cloud storage brings many conveniences to our lives andtechnological developments, it also faces various security threats. When the user delegates the cloud service provider to store the data.If there is no supervision mechanism for third party platforms, user data may bemaliciously tampered with or deleted by CSP. To solve this problem, an integrity auditingscheme for cloud storage data has been proposed. In the initial audit scheme, in order toverify the integrity of the data, users need to calculate and save the corresponding hashvalue of the data before upload the data to the cloud server (CS). By comparing the hashvalues, the user can determine whether the data stored on the cloud server is corrupted.However, as the number of data increases. Each time traversing the entire data for calculationincreases the computational complexity, reduces audit efficiency, and greatly increasescommunication costs.Most of the research now focuses on auditing data that can support dynamic modifications. In terms of data modification permissions, the original scenario onlysupports data owners to dynamically manipulate data. However, as the demand for shareddata increases, many auditing schemes are proposed to support group users to modify data.There are many audit schemes only consider how to verify the

integrity of data and the correctness of data storage.However, there is no corresponding protection for users' identity privacy when theysign data blocks. If the privacy protection of users' data is not taken into account, users datawill face the risk of leakage, which will cause security problems that cannot be ignored incloud storage and hinder the development of cloud computing.In 2010, Wang et al. proposed a scheme using the random mask and the public keybased authenticator technique to protect data privacy but does not support users to modifythe data. To protect the shared data from tampering and deletion, introduced a trusted thirdparty (TPA) to audit the data. It uses the idea of proxy re-signing to implement an effectiveuser revocation mechanism.In addition todata audit in cloud computing, there are also many other relevant12researches including fine grained access control, encrypted data search, identity based authentication and data crowd sensing.In the integrity auditing scheme of cloud storage data, implementing secure userrevocation ensures that data is shared among legitimate group users. More specifically, if therevoked user's access to data is not managed, then the CSP and revoked user will colludefor profit reasons, resulting in the corruption of data. Users in a group share the group private key to generate signatures.When a user is revoked, the group manager (GM) updates the group private key withoutdistributing the new private key to the user who needs to be revoked, and the remaining usersupdate their signatures according to the new group private key. But this approach can bringhuge overhead to communication and computing. Because of the process of generating asignature, the user needs to generate a signature again based on the messages stored in the cloud. In this project, we use the revocation list (RL) to manage the user's revocation, the tag is part of the signature, and the revoked user's tag is stored in the RL. When the user is revoked, the ability of the remaining users will not be affected. Since the tag generated bythe revoked user is invalid, the cloud server can reject the user access or update of the shared data after verifying the signature containing the invalid tag.

Data Storage:

Data stored on cloud servers is shared among legitimate group users. The shared data supports the user to modify it and other update operations. In order to prevent the collusion between revoked group users and CSP from leaking and tampering with shared data, we need to provide a secure user revocation mechanism while implementing efficient data audit. So we propose a shared dynamic data auditscheme with anonymous revocation of users.

The contributions are summarized as follows:

• Based on the dynamic user group, users in the group can be safely revoked.

• The proposed scheme supports the cipher text database being shared among multiple user,and the user has the right to modify data operation.

AES Algorithm and Ring Signature:

The more popular and widely adopted symmetric encryption algorithm likely to beencountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple-DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable to exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows:

• Symmetric key symmetric block cipher

• 128-bit data, 128/192/256-bit keys

• Stronger and faster than Triple-DES

• Provide full specification and design details

• Software implementable in C and Java

MODULES AND DESCRIPTION:

• Authentication

• Admin Add Users into Group

• Admin Generate Random Key to Users

• User Upload File

• Encrypt and Decrypt Uploaded File

• View File Using Random Key

• Download File

• Track Unknown User IP Address.

1. Authentication

The user first registers his/her own details like username, email, password and confirm password. After registration, he has to log in his own username and password. If the user name and is correct he has to go to his/her own account otherwise, it will give you an alert message Please Check Your User Name and Password.

2. Admin Add Users into Group

The admin adds registered users into a group. The admin generates random key for all group users individually. The random key should be forwarded to all group users. The users after getting permission from the admin. He logs into his own account. The user upload files, the files are encrypted and uploaded.

3. Admin Generate Random Key to Users

In this module, the admin generates random key to users. The admin generates random keys for every user in the group. The random key will be different from each and every user. The user can view another user files using this random key. The random key will be unique for each and every user in the group.

4. User Upload Files

In this module the user upload files in the group. The uploaded file will be encrypted and displayed in the group. The user can view files in the group using the random key that

is sent to admin. The user can download files in the group using this random key.

5. Encrypt and Decrypt Uploaded File

In this module, we can encrypt uploaded files. The uploaded files are displayed in the group and the files are encrypted.

6. View Friends Messages

In this module, we can view friend's messages. The Group is nothing but set of users who are connected to a specific group. In a group, we can send messages that can be viewed by set of friends who are in a group.

7. View Notifications

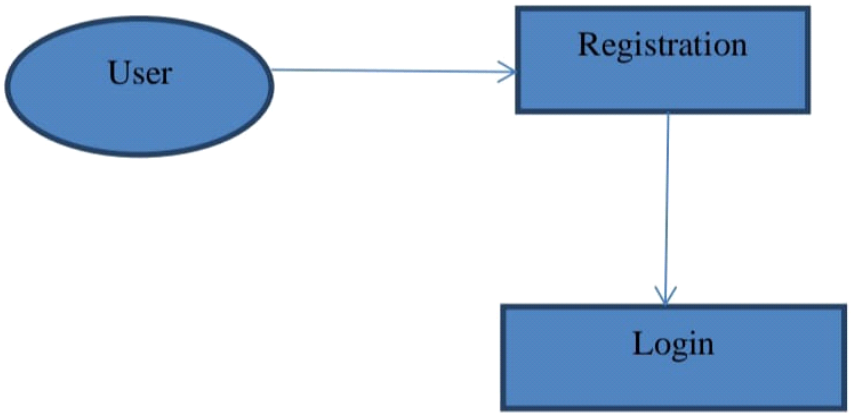
In this module, we can view upload images that are uploaded by friends and comments that are sent by friends. In notification page, we can view all comments to the specific image.

In notification page, the user also sends comment that is stored in a social network server. If suppose admin view server details.

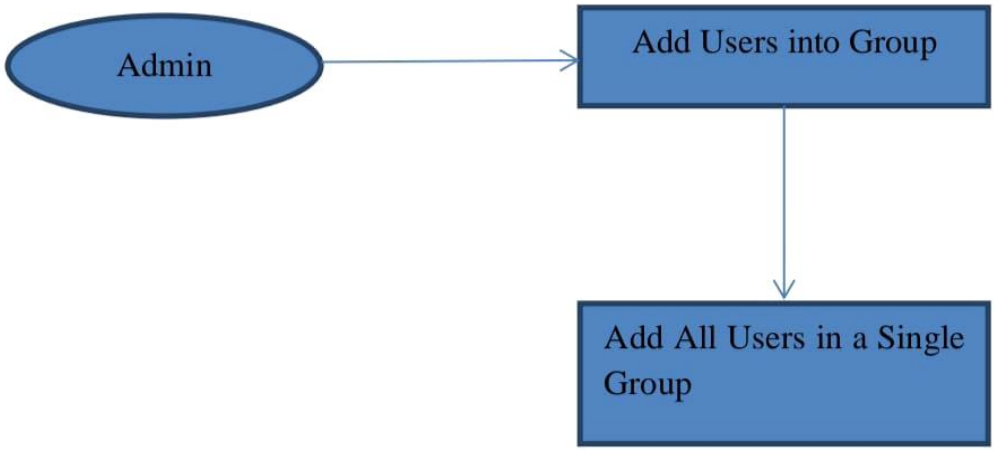
Admin can view user comments, Profile pictures, Group messages, and Notification and location details. This will lead to a threat to a social network user. In the Existing system, there is no security. In this proposed system we can encrypt user comments, Profile pictures, Group messages, Notification and location details are stored in the social network.

MODULE DIAGRAM :

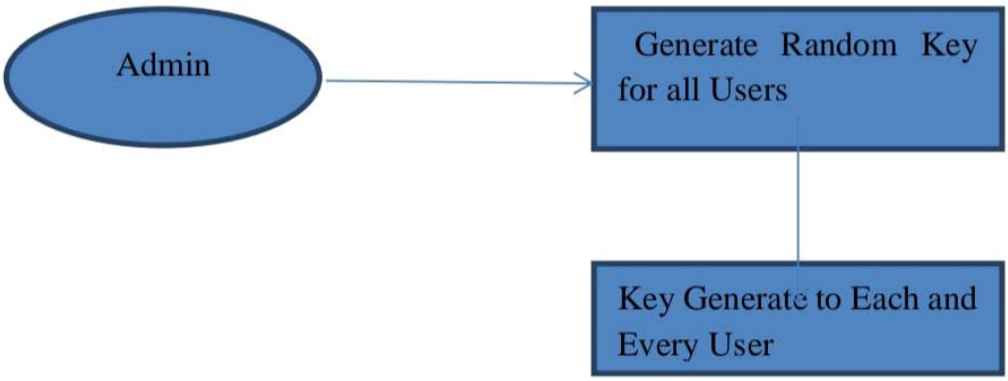
1. Authentication Process



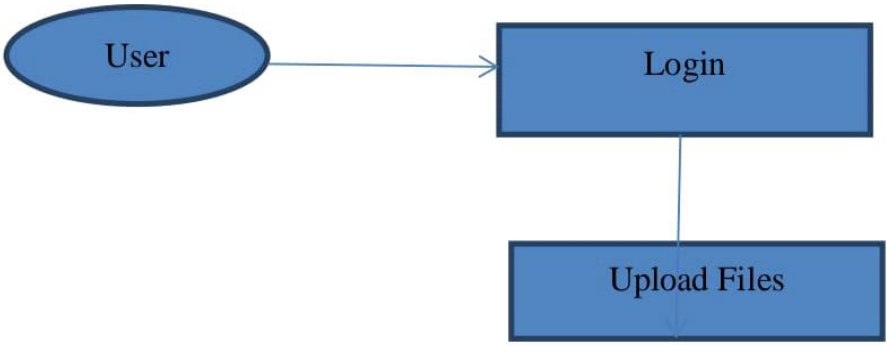
2. Admin Add Users into Group



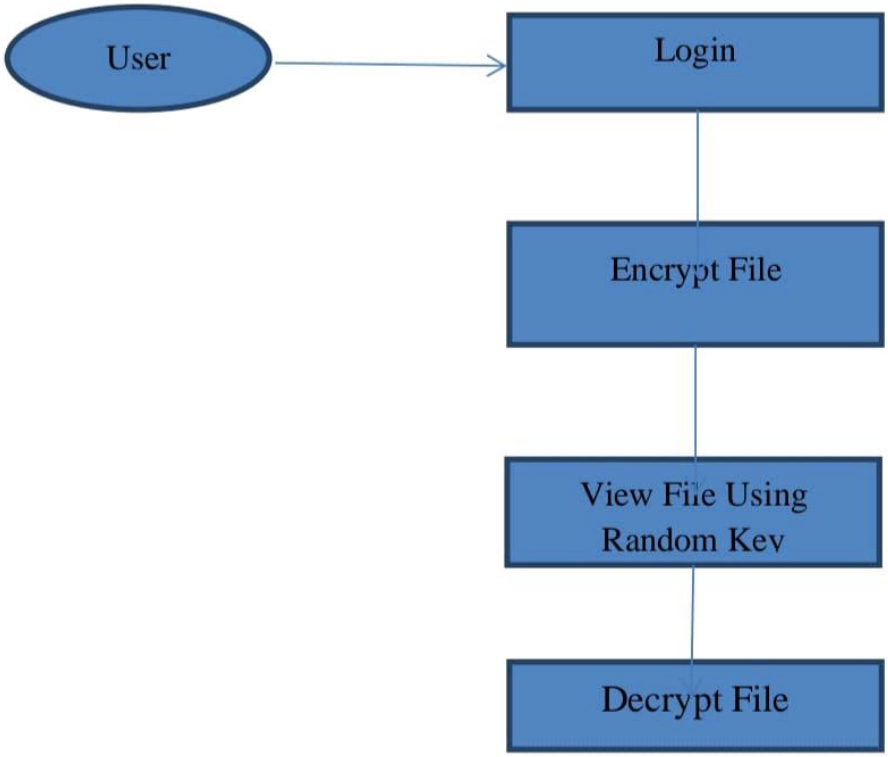
3. Admin Generate Random Key to Users



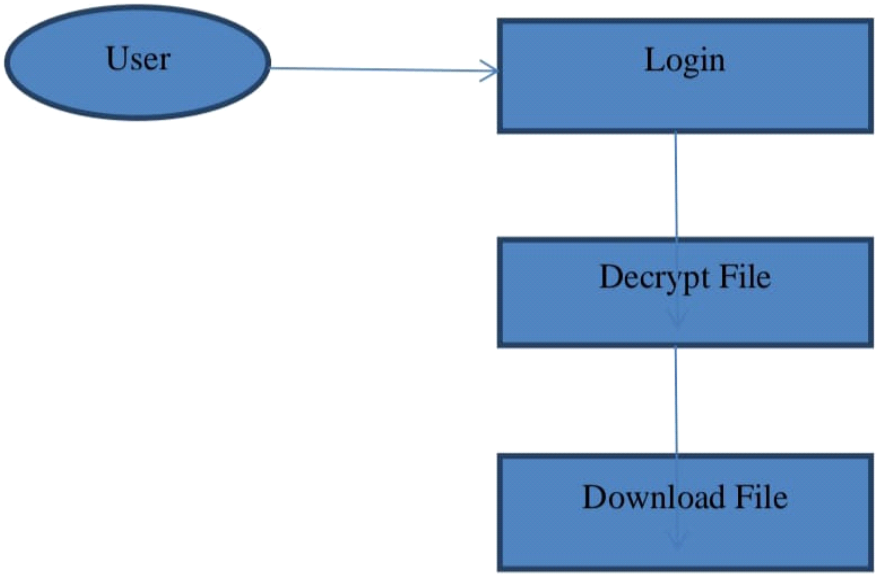
4. User Upload File



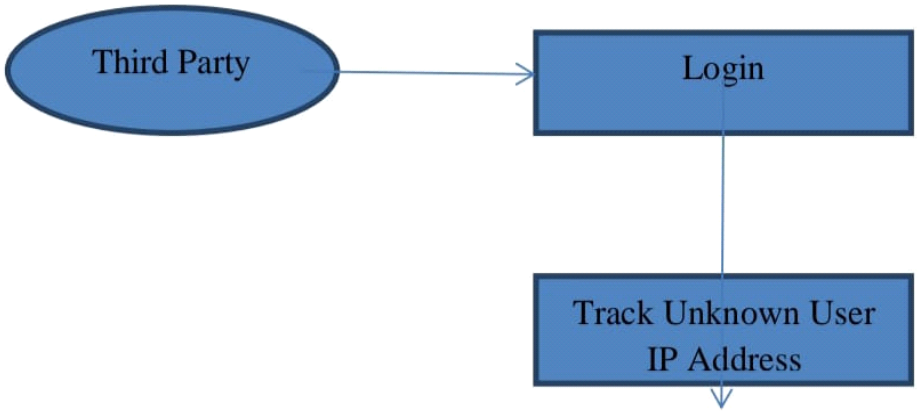
5. Encrypt and Decrypt Uploaded File



6.Download File



7. Track Unknown User IP Address



ENCRYPTION ALGORITHM:

1) Let G1, G2 are a bilinear group of order p (p - prime), g is generator group G1:

2) e: G1xG2G2 is bilinear mapping; d is a threshold value. The general scheme consists of four stages, for each of them has its own algorithm.

3) Generating the public key and master key Trusted centre selects randomly t1,...,in, y

from finite field Zq and calculates the public key PK=(T1=gt1,..., Tn=gtn, Y=e(g,g)y), where g is a bilinear group generator G1 of order p (p - prime). In this step, the master key is also generated MK=(t1,...,in,y).

4) Generate private keys A set of user attributes is supplied to the input of the private key generation algorithm, and the output of the algorithm turns user's pivate key.

The trusted centre generates a private key for each user U. AU is a set of user attributes. Randomly polynomial q of degree d-1 is selected such that is q(0)=y. Private key is D=Di=g(q(i))/(ti)IAU.

5) Encryption The input to the encryption algorithm is fed the message which it is necessary to encrypt, a set of attributes, the owner of which will be able to decrypt the data and randomly selected number, and the output of

the algorithm obtained encrypted data. Owner data encrypt a message M G2 using a set of attributes ACT and a random numbers Zq: CT=(ACT, E=MYs=e(g,g)ys, Ei=gtisiAU).

6) Description A set of user attributes AU and the encrypted data are supplied to the input of the decryption algorithm, and the output of the algorithm is obtained decrypted message. If—AUACT—d,thenofiAUACTselecteddattributes to compute values e(E,Di)=e(g,g)q(i)s,Ys=e(g,g)q(0)s=e(g,g)ys.

7) The original message is M=E/Ys. Private keys are generated in the scheme for the principle of secret sharing.

Input : Text File

Output : Encrypted File

Conclusion:

In this project, an efficient sharing auditing scheme for cloud storage data that supports anonymous revocation of users is proposed. By combining vector commitment primitives with an efficient signature scheme and key agreement protocol, we implement user security revocation and prevent collusion between the revoked user and the malicious cloud server. Our scheme supports dynamic changes in data and the joining or exiting of group members.

Stored data is not leaked to TPA or invalid users during auditing or sharing. Through the comparison of experimental results, our solution is effective and reduces the computational overhead of audit phases.

We propose a scheme to realize efficient and secure data integrity auditing for share dynamin data with multi-user modification. The scheme vector commitmen,Asymmetric Group Key Agreement (AGKA) and group signatures with user revocation are adopted to achieve the data integrity auditing of remote data. Beside the public data auditing, the combining of the three primitive enable our scheme to outsource cypher text database to the remote cloud and support secure group users revocation to shared dynamic data.

We provide the security analysis of our scheme, and it shows that our scheme provide data confidentiality for group users, and it is also secure against the collusion attack from the cloud storage server and revoked group users. Also, the performance analysis shows that, compared with its relevant schemes, our scheme is also efficient in different phases.

REFERENCES:

1. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, ‘‘Dynamic provable data possession,’’ in Proc. 16th ACM Conf. Comput. Commun. Secur., Nov. 2009, pp. 213–222.

2. P. S. Kumar, R. Subramanian, and D. T. Selvam, ‘‘Ensuring data storage security in cloud computing using Sobol sequence,’’ in Proc. 1st Int. Conf. Parallel, Distrib. Grid Comput. (PDGC), Oct. 2010, pp. 217–222.

3. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ‘‘Enabling public auditability and data dynamics for storage security in cloud computing,’’ IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011.

4. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, ‘‘Scalable and efficient provable\ data possession,’’ in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., Sep. 2008, Art.no. 9.

5. T. Jiang, X. Chen, and J. Ma, ‘‘Public integrity auditing for shared dynamic cloud data with group user revocation,’’ IEEE Trans. Comput., vol. 65, no. 8, pp. 2363–2373, Aug.\2016.

6. J. Yuan and S. Yu, ‘‘Public integrity auditing for dynamic data sharing with multiuser\modification,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1717–1726, Aug.2015.

7. C. Wang, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy-preserving public auditing for data storage security in cloud computing,’’ in Proc. IEEE Infocom, Mar. 2010, pp. 1–9.

8. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy- preserving public auditing for secure cloud storage,’’ IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375,Feb. 2013.

9. Y. Zhang, D. Zheng, and R. H. Deng, ‘‘Security and privacy in smart health: Efficient policy-hiding attribute-based access control,’’ IEEE Inter- net Things J., vol. 5, no. 3,pp. 2130–2145, Jun. 2018.

10. J. Sun, S. Hu, X. Nie, and J. Walker, ‘‘Efficient ranked multi-keyword retrieval with privacy protection for multiple data owners in cloud computing,’’ IEEE Syst. J., to be published. doi: 10.1109/JSYST.2019.2933346.

11. X. Chen, F. Zhang, W. Susilo, H. Tian, J. Li, and K. Kim, ‘‘Identity- based chameleon hashing and signatures without key exposure,’’ Inf. Sci., vol. 265, no. 5, pp. 198–210,2014.

12. Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, ‘‘Efficient and robust certificate less signature for data crowd sensing in cloud-assisted industrial IoT,’’ IEEE Trans. Ind. Informat., to be published.

13. D. Catalano and D. Fiore, ‘‘Vector commitments and their applications,’’ in Proc. Int. Workshop Public Key Cryptogr. Berlin, Germany: Springer, 2013, pp. 55–72.

14. T. Nakanishi and N. Funabiki, ‘‘A short anonymously revocable group signature scheme from decision linear assumption,’’ in Proc. Acm Symp. Inf., Comput. Commun. Secur., Mar. 2008, pp. 337–340.

15. Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, ‘‘Asymmetric group key agreement,’’ in Proc. Annu. Int. Conf. Theory Appl. Crypto- graph. Techn. Berlin, Germany: Springer, 2009, pp. 153–170.

16. L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, ‘‘Identity-based authenticated asymmetric group key agreement protocol,’’ in Proc. Int. Comput. Combinatory Conf. Berlin, Germany: Springer, 2010, pp. 510–519.

17. J. Yuan and S. Yu, ‘‘Efficient public integrity checking for cloud data sharing with multiuser modification,’’ in Proc. IEEE Conf. Comput. Commun., Apr./May 2014, pp. 2121–2129.

18. B. Wang, B. Li, and H. Li, ‘‘Panda: Public auditing for shared data with efficient userrevocation in the cloud,’’ IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92–106, Jan./Feb.2015.

19. De Caro and V. Iovino, ‘‘jPBC: Java pairing based cryptography,’’ in Proc. IEEE Symp. Comput. Commun. (ISCC), Jun./Jul. 2011, pp. 850–855.

20. G. Ateniese, R. C. Burns, R. I. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. Song, ‘‘Provable data possession at untrusted stores,’’ in Proc. 14th ACM Conf. Comput. Commun. Secur., Oct. 2007, pp. 598–609.