International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Lightweight Delegatable Proofs of Storage to Avoid Data Spillage using AVL Tree

Miss. Rajashri Bhongale[1], Dr. Arati Dandawate[2]
[1]PG student, [2]Associate Professor, Computer Department, JSPM's JSCOE, Savitribai Phule Pune University

Abstract: ***Cloud storage is associate progressively standard application of cloud computing, which might offer on-demand outsourcing data services for each organizations and people.Due to the information outsourcing, however, this new paradigm of knowledge hosting service jointly introduces new security challenges that desire associate freelance auditing service to check the information integrity inside the cloud.Some existing remote integrity checking ways that can exclusively serve for static archive knowledge and thus can't be applied to the auditing service since the information inside the cloud square measure typically dynamically updated.We consider the errand of allowing a Third Party Auditor (TPA), for the benefit of the cloud customer, to confirm the trustworthiness of the dynamic data hangs on inside the cloud. Proofs of storage (including Proofs of Irretrievability and demonstrable knowledge Possession) could be a cryptographic tool, that permits data owner or third party auditor to audit integrity of knowledge hold on remotely in Associate in Nursing extremely cloud storage server, while not keeping a region copy of data or downloading data back throughout auditing.***

Keywords: ***Multi-Cloud storage, Proof of Storage, Cloud Computing, Third Party Auditor***

I. INTRODUCTION

Cloud computing is extensively developed technology used in business, IT industries that provide services like network access, resources, infrastructure, platform, and speedy resource snap as per user need. The user will gain access of services anytime, anyplace on-demand. In cloud computing the info of user is centralized to the cloud storage. Many users from remote location use services incessantly thus there could arise some problems like information security, information integrity, dynamic updates. When it's inconceivable for user to test the info is being consistent that is hold on cloud storage. Thus user forever needs that cloud server should need to maintain information integrity and privacy. Cloud service suppliers are the separate entities that store information and supply services to the user.To ensure the information security and integrity and to cut back on-line burden it's of importance to change public auditing service for cloud storage, in order to audit the information. TPA wills the auditing method on behalf of the user.The TPA has capabilities and experience which will sporadically check the integrity of the info hold on in cloud. The user doesn't have the capabilities that the TPA has.

TPA keeps the data in original state and it also verifies the correctness performs this task by user permission. Enabling public auditing service will play an awfully vital role for privacy data security & minimizing the data risk from hackers. Documented capacity needs ensure with respect to the validness of learning on capacity, especially that capacity servers have learning. It's meager to find that information are adjusted or erased once getting to the data, because of it's going to be past the point where it is possible to recoup lost or broken information. Safe stockpiling servers hold gigantic measures of information, next to no of that are gotten to. They also hold information for extensive stretches of your time amid that there is additionally introduction to information misfortune from advertisement ministration blunders on the grounds that the physical execution of capacity advances, e.g., reinforcement and reestablish, information movement to new systems, and consistently changing enrollments in shared frameworks. To address the problems of existing publically verifiable POS schemes, we have a tendency to propose a replacement variant formulation referred to as Delegable Proofs of Storage (DPOS), that on one hand supports delegation of knowledge auditing task, like publically verifiable POS schemes, and on the opposite hand is as economical as a in private verifiable POS theme. Public verifiability of POS allows any third party auditor to check the original contents of data in cloud storage that considerably eliminates the burden of knowledge owner. A theme that supports delegation of knowledge similarly because it is economical as POS in in private verifiable scheme is DPOS.

AVL tree can be a tree throughout that distinction between heights of sub-trees can not be quite one for all the nodes. In projected system, we've a bent to are visiting apply this concept of AVL tree to check the integrity of the users data that's hold on cloud. If there's modified in information, that we'll verify victimization third party auditor. It checks for original content and can show acceptable message to user. To produce additional security, we have a potential to are visiting divide the information files into

blocks and going to use double encoding by victimization 2 algorithmic programs Bastion and changed RSA algorithm, initial we'll inscribe the information victimization Bastion and ciphertext are going to be re-encrypted using changed RSA algorithmic program. So info is going to be safer as twin encoding is given in projected system. Once we have a tendency to get twin encrypted ciphertext, it'll be divided in blocks and theses blocks are going to be keep on totally different servers. Similarly as once secret is generated it will even be divided in blocks to remain it safe from somebody, as he got the encryption key he can get only key thus attack will not be taken place and data won't be disclosed and might be extra secured. Planned Bastion and adjusted RSA formula, a subject that ensures the confidentiality of encrypted information even once the somebody has the cryptography key, and every one however re-encrypted ciphertext blocks. Bastion is best suited to settings wherever the cipher text blocks are hold on in multi-cloud storage systems and adjusted RSA generates long bit cryptography key thus information ought to keep secure even the somebody tries to rewrite it. To boot as cryptography key are divided and may be hold on within the blocks for additional security.

II. RELATED WORK

Proofs of storage (including Proofs of Retrievability and obvious knowledge Possession) could be a cryptographic tool, that allows data owner or third party auditor to audit integrity of knowledge keep remotely in an exceedingly cloud storage server, while not keeping a neighborhood copy of knowledge or downloading data back during auditing. Delegatable proofs of storage permits information owner to delegate auditing task to a 3rd partyauditor, and in the meantime retains the aptitude to perform audit task by her, whether or not the audit or colluded with the cloud storage server. Our formulation additionally support revoking and shift auditors evidently[1].

The client keeps up a continuing with quantity of data to substantiate the confirmation. The test/reaction convention transmits a touch, consistent live of learning, that limits prepare correspondence. During this manner, the PDP show for remote knowledge checking underpins huge data sets in usually circulated capability frameworks. We tend to blessing two provably-secure PDP plans that are more cost-effective than past arrangements, even analyzed with plans that succeed additional fragile certifications. Especially, the overhead at the server is low (or even steady), as operation bestowed to straight within the span of the data [2].

Numerous capability frameworks rely on replication to broaden the accessibility and strength of learning on untrusted storage frameworks. At present, such capability frameworks provide no solid proof that varied duplicates of the information are actually put away. Capability servers can decide to form it look like they are golf shot away some duplicates of the data, while inreality they completely store one duplicate. We tend to handle this deformity through various copy demonstrable data possession(MR-PDP): A provably-secure set up that allows a client that stores t reproductions of a document during a capability framework to substantiate through a take a look at reaction convention that (i) all of a form reproduction will be created at the season of the take a look at and that (ii) the capability framework utilizes t times the capacity neededto store a solitary copy [3].

By utilizing Cloud storage, shoppers will get to applications, administrations, programming at no matter purpose they needs over the net. Shoppers will place their info remotely to distributed storage and find advantage of on-request administrations and application from the assets. The cloud should have to guarantee information uprightness and security of knowledge of consumer. The difficulty concerning distributed storage is honourableness and protection of knowledge of consumer will emerge. to remain up to unneeded excess this issue here, we have a tendency to are giving open reviewing method for distributed storage that shoppers will create utilization of an outsider examiner (TPA) to test the trait of knowledge. Not simply confirmation of knowledge honourableness, the projected framework in addition underpins info components. The work that has been drained this line desires info components and real opens auditability. The inspecting endeavor screens info alterations, additions and erasures [4].

We think concerning the difficulty of proficiently demonstrating the honesty of knowledge put away at untrusted servers. Within the obvious info possession (PDP)show, the client preprocesses the knowledge associate degreed afterward sends it to an untrusted server for capability, whereas keeping a bit live of data. We gift a definitional structure and effective developments for dynamic obvious info possession (DPDP) that expands the PDP model to assist obvious updates to place away info. We have a tendency to utilize anew variety of valid word references captivated with rank knowledge [5].

Confirmations of capability (CoS) are intuitive conventions sanctioning a client to test that a server firm stores a record. Past work has incontestable that evidences of capability are often developed from any homomorphic straight appraiser (HLA). The latter, generally, are mark/message confirmation plans wherever 'labels' on varied messages are often homomorphically consolidated to yield a 'tag' on any direct we have a tendency to at that time tell the simplest thanks to rework any open key HLA into a freely simple PoS with correspondence varied nature autonomous of the le length and supporting AN limitless variety of confirmations [6]. Information administrations for the 2 associations and other people. Notwithstanding, purchasers might not fully believe the cloud specialist co-ops (CSPs) in that it's exhausting to determine if the CSPs live up to their lawful wishes for info security. During this

manner, it's basic to form proficient reviewing strategies to fortify info proprietors' trust and trust in distributed storage. during this paper, we have a tendency to gift a unique open examining set up for secure distributed storage passionate about distinctive hash table (DHT), that is another two-dimensional infostructure placed at a 3rd equality examiner (TPA) to record the knowledge} property data for dynamic inspecting. Variable from theexisting works, the projected set up moves the approved information from the CSP to the TPA and during this manner primarily diminishes the process expense and correspondence overhead. Within the interim, misusing the fundamental preferences of the DHT, ourplan will likewise accomplish higher refreshing productivity than the simplest at school set ups [7].

Distributed computing has been notional because the leading edge engineering of IT Enterprise. It moves the applying Programming and databases to the brought along large server farms, wherever the administration of the knowledge and administrations might not be utterlydependable. This novel worldview achieves varied new security challenges, that haven't been for certain knew. This work examines the difficulty of guaranteeing the honourableness of data storage in Cloud Computing. Specifically, we expect regarding the enterprise of allowing a 3rdparty examiner (TPA), within the interest of the cloud client, to test the honourableness of the dynamic data place away within the cloud. the assistance for data components through the foremost broad kinds of informationactivity, for instance, sq. alteration, addition, and cancellation, is in addition a stimulating advance toward reasonableness, since administrations in CloudRegistering don't seem to be restricted to file or reinforcement data because it were. Whereas earlier chips away at guaranteeing remote data uprightness of times doesn't have the assistance ofeither open auditability or dynamic data tasks, this paper accomplishes each [8].

In spite of the actual fact that the benefits are clear, such Associate in nursing administration is likewise surrendering clients'physical possession of their decentralized info that ineluctably presents new security dangers toward the accuracy of the data in cloud. Inrequest to handle this new issue and any accomplish a secure and trustworthy distributed storage administration, we tend to propose during this paper a adaptable sent warehousing honorableness inspecting system, victimization the homomorphic token and disseminated obliteration coded info. The proposed configuration allows purchasers to review the distributed storage with exceptionally light-weight correspondence and calculation value. The reviewing resultensures solid distributed storage accuracy guarantee, nonetheless additionally at the identical time accomplishes fast info mistake limitation, i.e., the ID of acting naughtily server [9].

Due to the knowledge redistributing, be that because it could, this new worldview of data facilitating administration likewise presents new security challenges, which needs associate autonomous reviewing administration to test the knowledge honesty within the cloud. Some current remote trustiness checking methods will serve for static document information and consequently cannot be connected to the reviewing administration since the knowledge within the cloud is increasingly invigorated. Consequently, an efficient and secure dynamic evaluating convention is needed to influence info proprietors that the knowledge are accurately place away within the cloud. We have a potential to 1st arrange a reviewing structure for distributed storage frame works what's a lot of, propose a skilled and protection safeguarding examining convention. At that time, we have a tendency to stretch out our reviewing convention to assist the knowledge dynamic tasks, that is skilled and demonstrably secure within the irregular prophet demonstrate. We have a tendency to more broaden our examining convention to help cluster reviewing for each varied proprietors and various mists, while not utilizing any confided in arranger. The investigation and recreation results demonstrate that our projected reviewing conventions are secure and skilled, notably it reduce the calculation price of the examiner [10].

III. PROPOSED ALGORITHM

A. Description of the Proposed Algorithm:

1) Data Owner

a) Data owner generate public keys.

b) Data owner will be responsible for encrypting files and generating authentication tags also.

c) Data owner will upload all this data to cloud.

2) Cloud Service Provider

a) Cloud service provider will store all the data i.e. file along with keys and authentication tags.

b) Cloud Service Provider will work according to the request and response from the user.

3) ODA

a) Verification of file content is done by ODA.

b) Check for integrity.

4) Data User

a) Data user will request for keys to the Data Owner.
b) Data Owner will send keys to the Data user.
c) With keys he can decrypt and download the original content of the file.

5) Pseudo Code

File Splitting, Encryption and Decryption:

a) Input: Text file, secret key
b) Output: Encrypted Files E (F.1), E (F.2), E (F.3), E (F.4), and E (F.5), Decrypted files.
i) Step 1: Divide the file into blocks.
ii) Step 2: Uploads a file (F) and secret key (SK)
iii) Step 3: Index based files (F.0, F.1, F.2, F.3 and F.4) are created with the same file name.
iv) Step 4: Encrypt each part of the divided file E (F.1), E (F.2), E (F.3), E (F.4), and E (F.5) and upload it to the Cloud server.
v) Step 5: Provide keys to the to the ODA i.e. Third Party Auditor.
vi) Step 6: ODA will choose the file along with verification key pair and upload it to the cloud.
vii) Step 7: Data user will request for keys to Data Owner and once have them can decrypt and download the file.
viii) Step 8: Enter the File Name (FN) and Secret Key (SK) from the data owner or File owner by making request
ix) Step 9: Perform a search with the filename associated in Cloud storage service provider directory (F.0, F.1, F.2, F.3 and F.4)
x) Step 10: Pass the secret key (SK) to the data user
xi) Step 11: Data user can download the original file F.
xii) Step 12: End.

IV. SIMULATION RESULTS

In this proposed system, we are re-encrypting user's data so providing more security to user's data. When it comes to comparison between existing and proposed system, the time required to encrypt and decrypt users data is the main factor. Proposed system takes less time as compared to existing system. In proposed system the users data is divided into multiple blocks and to each block there is one tag assign, with this security we are uploading users data on cloud, but even if with this also, any attacker gets access to any file , he cannot stole data, because the data will be stored on different clouds.The average time taken for encryption and decryption of data is more as compared to proposed system in existing system while proposed system takes less time to encrypt data.In existing system time required to encrypt and upload data on cloud is more while in proposed system the time required to encrypt data and upload it to cloud is less as compared to existing system. To download uploaded file from cloud is also fast with proposed system.

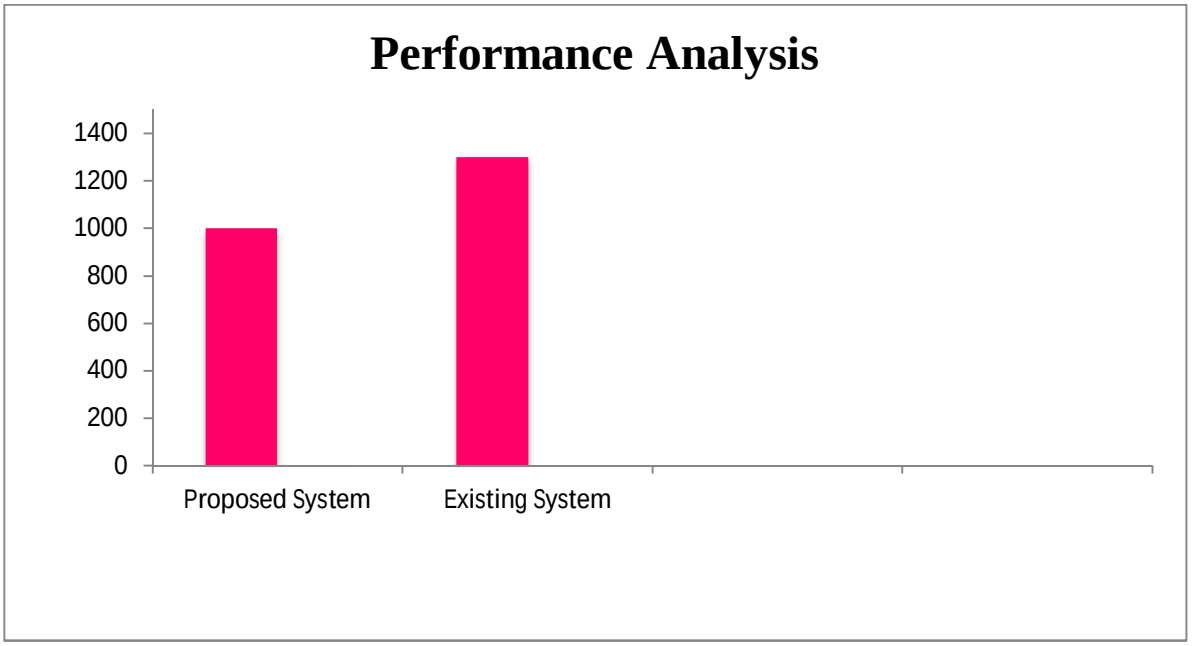

Fig.1. Performance analysis for 1 MB file

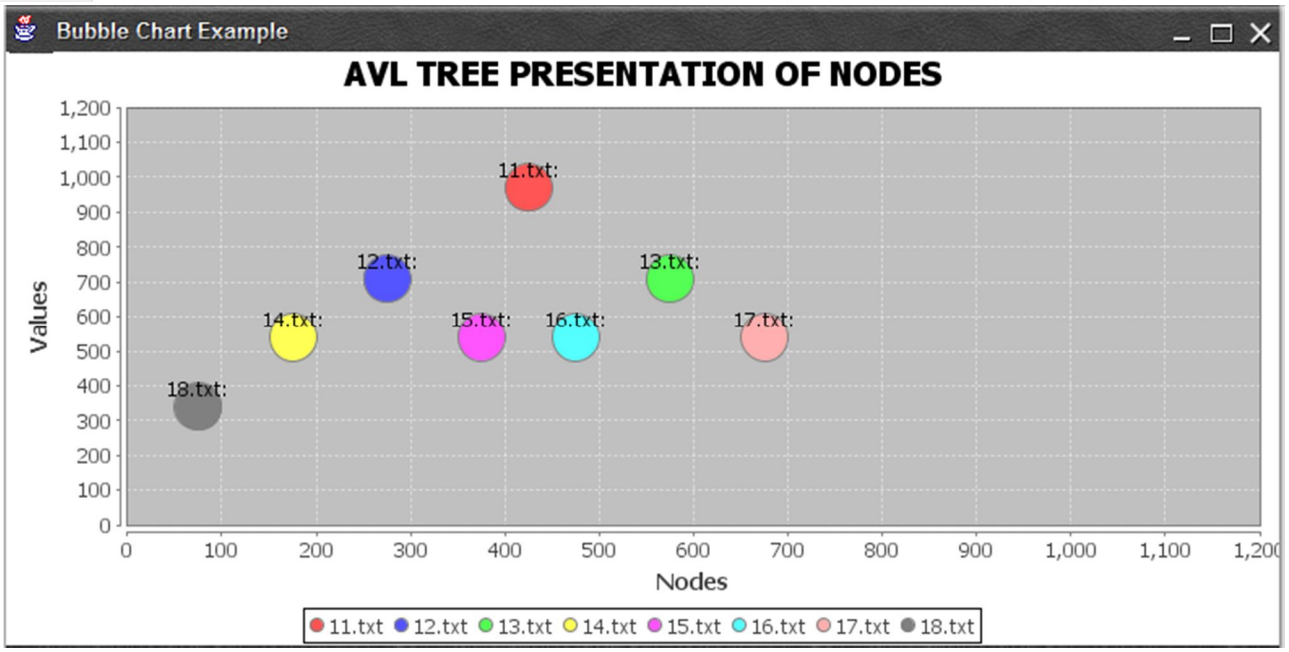

Fig 2. AVL Tree Presentation of Nodes

V. CONCLUSION AND FUTURE WORK

Propose system provides security to the user knowledge by taking users data, the data i.e. file are going to be divided into totally different blocks. Then, these blocks are encrypted by applying 2 totally different algorithms i.e. changed RSA and Bastion algorithmic program. Through these algorithms we tend to are re-encrypting user's knowledge. Once this the information owner is going to be chargeable for generating the combine of various keys like public and secret key. The divided components of the files can have totally different tags, this tags also will be created by the information owner. Then all knowledge together with file is going to be uploaded to cloud. Cloud service supplier provides the acceptable knowledge, tags and key combine as per the request from totally different users like knowledge owner, data user, and ODA. Here ODA can check for integrity of the user's knowledge, and if there are some changes in content then the acceptable message are going to be given to the user. Knowledge user request for keys to the ODA and gets the keys are going to be ready to rewrite and transfer the file. With this we tend to are ready to give additional security to user's knowledge, execution time of the planned system is additionally economical.

REFERENCES

[1] J. Xu, A. Yang, J. Zhou, and D. S. Wong, "Lightweight Delegatable proofs of storage," in Proceedings of 21st European Symposium on Research in Computer Security, ESORICS 2016, pp. 324–343, Springer International Publishing, 2016.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 598–609, ACM.
[3] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in Proceedings of the 28th International Conference on Distributed Computing Systems, ICDCS 2008, pp. 411–420, IEEE, 2008.
[4] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Transactions on Computers, TC 2013, vol. 62, no. 2, pp. 362–375, 2013.
[5] C. C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," ACM Transactions on Information and System Security, vol. 17, pp. 15:1–15:29, April 2015.
[6] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Advances in Cryptology -ASIACRYPT 2009, vol. 5912 of LNCS, pp. 319–333, Springer, 2009.
[7] Hui Tian, Yuxiang Chen, Chin-Chen Chang, "Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage," IEEE TRANSACTIONS ON SEVICE COMPUTING, MANUSCRIPT ID
[8] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011
[9] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 5, NO. 2, APRIL-JUNE 2012
[10] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Advances in Cryptology -ASIACRYPT 2009, vol. 5912 of LNCS, pp. 319–333, Springer, 2009

[11] I. G. Aniket Kate, Gregory M. Zaverucha, "Constant-Size Commitments to Polynomials and Their Applications," in Advances in Cryptology - ASIACRYPT 2010, pp. 177–194.
[12]] J. Alwen, Y. Dodis, and D. Wichs, "Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model," in CRYPTO '09: Annual International Cryptology Conference on Advances in Cryptology, pp. 36–54, 2009.
[13] Dan Boneh, Ben Lynn, and HovavShacham, "Short Signatures from the Weil Pairing," J. Cryptology (2004) 17: 297–319
[14] G., Burns, R., Curtmola, R., Herring, J., Khan, O., Kissner, L., Peterson, Z., and Song, "Remote Data Checking Using Provable Data Possession," ACM Trans. Info. Syst. Sec. 14, 1, Article 12
[15] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 584–597, ACM, 2007.
[16] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology - ASIACRYPT 2008, vol. 5350 of LNCS, pp. 90–107, Springer, 2008.
[17] B.Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in Proceedings of 5th International Conference on Cloud Computing, Cloud 2012, pp. 295–302, IEEE, 2012.
[18] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," in CRYPTO '92: Annual International Cryptology Conference on Advances in Cryptology, pp. 31– 53.
[19] J. Alwen, Y. Dodis, and D. Wichs, "Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model," in CRYPTO '09: Annual International Cryptology Conference on Advances in Cryptology, pp. 36–54, 2009.
[20] Jiawei Yuan, Shucheng Yu, and Song, "Proofs of retrievability with Public Verifiability and Constant Communication Cost in Cloud," ACM Trans. May 8, 2013, Hangzhou, China.
[21] Dan Boneh, Ben Lynn, and HovavShacham, "Short Signatures from the Weil Pairing," J. Cryptology (2004) 17: 297–319