Research Article

Active auditing Services for Storing and Securing the Data in the Cloud

Vidhya.G[a*],Basker.N[a],Dhaynithi.J[a], Marimuthu.M[a], Theetchenya.S[a], Vidyabharathi.D[a], Mohanraj.G[a]

[a]Sona College of Technology, Department of Computer Science and Engineering, Salem, Tamil Nadu

*gvidhyacse@gmail.com, bas2k9@gmail.com, dhaya.j@gmail.com, mari.btech@gmail.com, theetchenya@gmail.com dvbharathi77@gmail.com, mohanraj134@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Cloud computing paradigm is a variation on the long vision of computing as utilisation of resources, in which data owners can host all data tenuously in the cloud and access high-quality software products on demand from a mutual pool of configurable computing resources. We create a secure storage system to alleviate data owners' burdens and to remove their substantial control over storage reliability and security, we develop a secure data storage services with high service-level requirements. Our proposed one involves three favors: the cloud server, data owner and TPA. The pros and cons of cloud computing are examined in this paper and then we put a set of analytically and cryptographically desirable properties allowing large data storage security audit services to become a authenticity. Active auditing is required to check the dynamic data integrity. But it's not easy to do an audit effectively, since data is complex in the cloud. To fail the auditing process, server will implement replay attack and forge attack. Modification, insertion and deletion comprise the complex operations. The owner sends the update message to the auditor any time the complex operation is performed. Built on the techniquepart structure, random case and Dynamic-Hash Table(DHT), our audit service can support validated improvements to externalise the data, and timely abnormal detection.

Keywords: Cloud Server, Data Owner, TPA, Cryptographic Primitives, DHT(DHT), Data Security

1. Introduction

Cloud storage area space is an important in cloud computing framework that subject to provide reliable data transfer services on the side when it is needed by user with highly virtualized infrastructure. Cloud storage area, which is cost effective and high performance, is encouraging more and more enterprises and individuals to externalise data storage to expert Cloud Service Provider (CSPs), which is motivating the fast development of cloud storage area. As new technologies evolve, cloud storage area space still faces many security challenges. One of the most important issue is ensuring g the legal compatibility of the cloud storage area system and the service provider. This is mainly focussed with the following reasons.

To begin with, cloud user who externalise their data to cloud is no longer able to check the quality of the data using standard methods that are commonly used in local storage scenarios. Second, CSPs that experience Byzantine Failure([1-3] from time to time can choose to cover data errors from data owners for their own benefit. What's more concerning about here is that, in order to save storage space, CSPs can fail to retain or even remove infrequently accessed data belonging to normal customers. Data stored in an untrusted cloud, on the other hand, is subject to suspicion and scrutiny, as data can easily be lost or compromised due to hardware failures and human error. In order to preserve the credibility of cloud data, open auditing is better done by adding a TPA, which provides its auditing service with more efficient processing and communication capabilities than standard user.

The Public Data Possession (PDP) tool for account credentials is considered to check the integrity of data store on an insecured network not including having to retrieve any of the data. Going forward, Wang et al. proposed to create aopen cloud data audit. In the future, Wang et al. intend to develop a public cloud data audit framework that keeps the accuracy of a user's private data hidden from a third-party auditor during open auditing. Therefore, it is crucial and necessary to establish effective auditing techniques to enhance the trust and confidence of data owners in cloud storage area, the core in which is how data integrity can be effectively verified remotely.

To date, numerous solutions to this problem have been suggested, which can be categorised into two categories: secretlyown auditing and common open auditing. Secret auditing is the primary model for distant data integrity testing in which the testing process is carried out openly between data owners and CSPs. But it can't produce compelling audit results, as owners and CSPs sometimes distrust each other. In addition, user are advised not to check frequently as the additional cost increases. For this reason, for the first time, a general test system was introduced, and its performance is usually evaluated by a TPA. Compared to the first case, the second case provides reliable test results and reduces the unnecessary burden of having to provide an independent TPA to the user.

Privacy protection

Data privacy has always been a major concern when it comes to cloud computing. Really seek to define would protect user' privacy when enforcing a TPA is at the heart of this problem in open auditing. Although using data encryption before outsourcing will help to ease privacy concerns in cloud storage area, it cannot stop data outflow during the testing process. For cloud auditing, it is therefore important to provide a privacy mechanism that is independent of data encryption.

2. Related Works

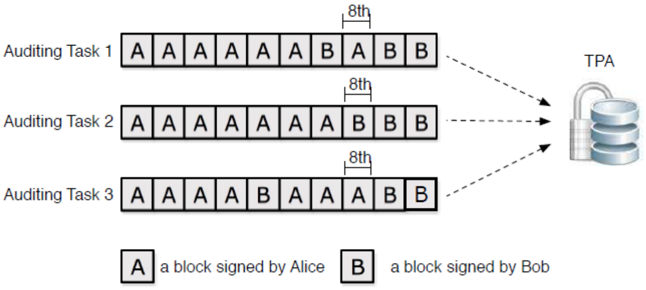
Group auditing

A TPA can holdnumerous audit tasks where different user would gain in a cost-effective approach i.e. support batching auditing, to increase efficiency and enable open auditing to be scalable[4-15].

Active auditing Since it is fit understood that a cloud storage area system is more than just a statistics centre, user must be able to dynamically modify data to meet the needs of various applications. We agree that data sharing between severaluser is one of the most appealing features of cloud storage area. Since the identities of signers on pooled data may mean that a particular user in the group or a special block in pooled data is a more desirable target than others, a specific issue raised during the public audit process for pooled data in the cloud is how to protect the TPA's privacy of identity. For example, UserA and user Bcollaborate as a set and split a cloud-based file.

The sharing folder is separated into several smaller files, each of which must be signed separately by each user. If a group member modifies a block in this collective file, the new block must be signed with their private key[16-20].The TPA requests to identify the signer 's identity on-block in this collective file, so it can inspect the credibility of the entire file based on UserA or UserB's requests.

Figure.1 After UserA and user Bshare a file in the cloud, the TPA audits the data's integrity using existing processes



After several audit activities have been completed, any private or confidential information may be revealed to the TPA. On the one side, UserA signs the majority of the blocks in the collective file, implying that she holds a leadership role in the party. On the erstwhile , 8th block is regularly changed by different user. This means that this block will contain high-value data, such as an auction final bid, which UserA and user Bwill need to negotiate and alter several times. The identities of the signers on pooled data, as discussed above, may mean that the user is a more valuable target than others in the group or block in pooled data. However, no existing system in the literature can perform open auditing of pooled data in the cloud while maintaining identity privacy.

Moreover ,Cloud storage area is an widely accessed in cloud computing technology which can provide on-demand data hosting services for organization and persons alike. On the other hand, consumers do not have total belief in the CSPs as it is difficult to assess if the CSPs meet their legitimate data protection requirements. Therefore, the implementation of successful auditing techniques is crucial to increasing the trust and confidence of data owners in cloud storage area.This paper proposes a novel secure cloud storage area public audit scheme based on a DHT[21-24], which is a modern two-dimensional data structure located in the TPA to record attribute information dynamic audit data. The proposed scheme, in comparison to current works, acumulates the approved in sequence from the CSP to the TPA, greatly reducing overhead computational costs and communication cost.. In the meantime, taking advantage of the DHT's technical advantages, our scheme can also achieve greater efficiency in updating than the state-of-the-art schemes.

And also extending this project to help privacy protection by combining the public key-based homomorphic authenticator with TPA-generated random masking, and it achieve group auditing by using the aggregate BLS signature technique. Here systematically demonstrate the safety of the proposed scheme and assess the efficiency of the audit through detailed tests and comparisons with current ones. The results show that the proposed scheme can effectively achieve safe cloud storage areaaudit, and outperform previous schemes in computational complexity, cost of storage and communication complexity.Introduction of an authenticated data structure to achieve Active Auditing(AA) is common. Typical members are the PDP based on the skip list, and the MHT-based public audit scheme. They will however incur high TPA computing costs and large overhead communication during the processes of updating and verification. As a result, Zhu et al. created an Index Hash Table (IHT) to monitor data block changes and aid in the generation of each block's hash value during the verification process. The IHT structure is a 1-d array that includes an index numeral, numeral of columns, numeral of variants and a random value.

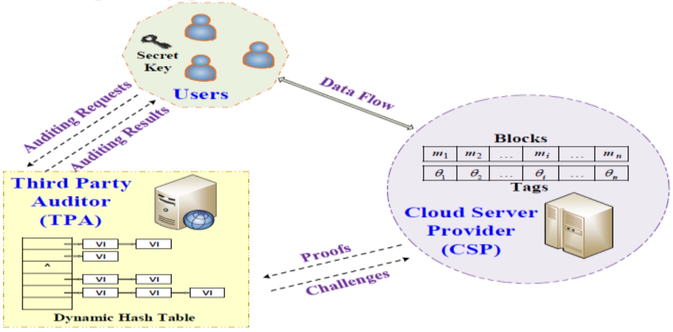
Through using the IHT inside the TPA in its place of the CSP to store data properties for auditing, IHT-based scheme can also decreasecomputational cost and communication cost. Unfortunately, since the mean of n/2 elements changes, the update process (especially inserts and deletes) is inefficient due to IHT's IHT array structure. The total number of blocks is n. When adding or removing, be sure to include the block number to ensure the right block name. During the redesign and testing phases of existing projects, TPA measurements and message overhead are included. IHT is critical to IHTPA's data active support, but it is unproductive in updating operation, especially inclusion and removal. This is clearly inefficient and would lead to higher computing costs.

3. Proposed Method

Data store in the cloud can access from one place at any time, as long as network access is available. storage space maintenance task, such as buying extra storage competence, can be offloaded to a service provider 's responsibility. The data sharing between user is another benefit of cloud storage area. If UserA wants to share some data (e.g. a video clip) with UserB, the amount of data can cause problems with sending emails. Instead, UserA uploads the file to the cloud storage area system so that UserB can restore it at any time. At the same time, externaldata storage increases the possibility of attack. For example, the more locations it is stored, the greater the risk it contains for unauthorized physical access to the data, when the data is distributed. By sharing the resources, string the data via networks with a lot of difficulties with other user and in turn an unauthorized user can also access personal data. This can also due to wrong actions, damaged equipment or, at times, criminal intent. A promising solution to offset the risk is to deploy encryption technology and use the Auditing technique and this could be very useful in preventing the attackers and hijackers from data.

Proposed system engages with the normal cloud setup with, for example, AWS with the CSP providing easy deployment with the cloud of the projects. Setting up a third-party auditor who works as a mediator between the client and the cloud server, performing audits that are confidential between the cloud and the server.From fig 2 the DHT. Serve the purpose with the auditor, and with the help of key initiation, provide security.

Figure.2 Architectural Design for auditing the cloud


Secret Key
Users
Data Flow
Auditing Requests
Auditing Results
Blocks
m_1 m_2 ... m_i ... m_n
θ_1 θ_2 ... θ_i ... θ_n
Tags
Third Party Auditor (TPA)
Cloud Server Provider (CSP)
VI
Dynamic Hash Table
Proofs
Challenges

The Client who creates account with the cloud and by using the login credentials, the user gets approval by the auditor and registers the account with the auditor and then the client uploads and downloads the file after the encryption and decryption done by the Security Device Issuer.

3.1 Third Party Auditor (TPA)

It acts as the mediator for both the Client user and the CSP. A TPA provides auditing setup with the help of the data structure hash table which updates automatically. The hash table which holds the key label through which the files can be uploaded or downloaded. The TPA works under the principle of the Block authentication code algorithm (BAC).

3.2 Cloud Server

The Cloud server where the client stores their data and uses it wherever they are. The Organizations provide cloud services act as server and allow their servers to store the data. The file a bond with the clients and allow their space to share with clients to store data.

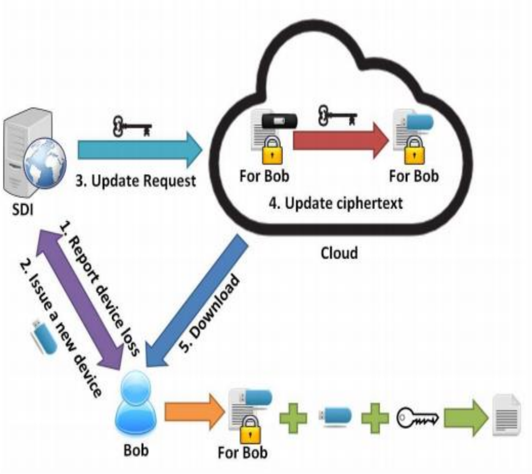
3.3 Client Registration

The client is allowed to create the account by providing some of the user details such as the ID which depends upon the user and then the Username and the password for their account. The client when contacts the cloud, they should decide whether to download or upload the file. This provides client registration for both sender and the receiver. It retains activation of the user until aTPA provides access thus permits for approval of the clients.

3.4 Security Device Issuer

The Security device issuer initializes the key block mechanism and grants the permit access to the clients registers with the cloud and the security device issuer allows the files to get encrypted and then the files secret key can be generated. The work of the security device issuer can be illustrated by the following fig 3.

Figure.3 Security device Issuer



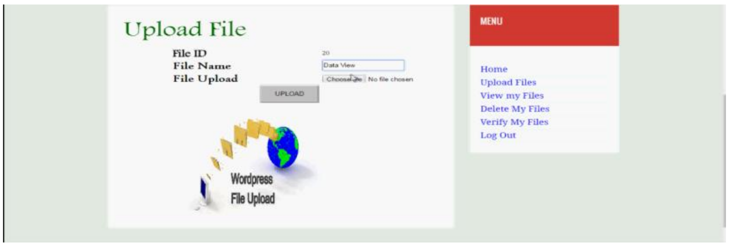
3.5Cryptographic Techniques for Security

Dynamic verification and privacy protection can be done for initiating key setup and the verification. Once the permission to the file is granted the file can be encrypted with the cryptographic encryption techniques known as the Block Authentication Code algorithm through which the file is proceeded with the encryption technique which allows the file contents can be divided into the block and a key index can be assigned to the block for the identification of the block then the secret key can be given to block, with the help of the secret key the block can be altered and the files can be modified and deleted only if the file contains the corrupted message. Finally proof check for the files can be done by the TPA by verifying all the hash values assigned to the block. The hash values can be stored in the variable vi which can used for the further reference.

4. RESULTS AND DISUSSIONS

The proposed system that works with novel audit system, whichcan support complex data operation and appropriate abnormal detection with the help of several successful techniques such as fragment structure, random sampling, and DHT. In addition, to improve the quality of audit services, here proposed a revolutionary approach based on probabilistic inquiries and periodic verification.A proof-of-concept framework is also being introduced to assess the feasibility and efficacy is compared wuthproposed methods. Our findings not only confirm the efficacy of our methods, but also indicate that our system has lower computational costs and needs less extra storage for integrity verification. There are several drawbacks to the new scheme. Static auditing is insufficient for Cloud data due to its dynamic existence. To ensure the integrity of dynamic data, Active auditing is required. However, due to the complexity of data in the cloud, conducting an effective audit is difficult. The server can use replay and forge attacks to fail the auditing procedure. Modification, addition, and deletion are examples of dynamic operations.When a complex process is completed, the owner sens an update message to the auditor, along with the message's index number. The Auditor is the one who keeps the tab up to date. The message m and tag are replaced by the new message and tag in message change. A new message m and a new tag are inserted during the insertion phase.Message m and tag are removed from the hash table for the dynamic block, and all entries below the deleted message move upwards.

Figure.4 Upload a File

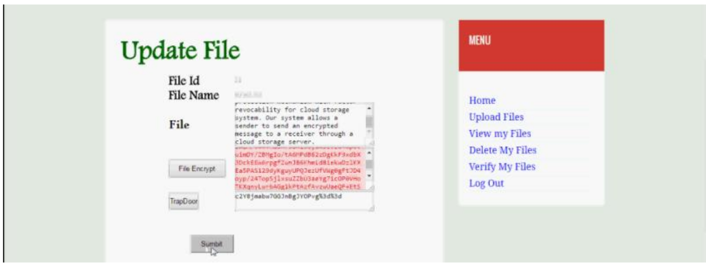

Upload File

File ID 20

File Name Data View

File Upload Choose file No file chosen

Figure.5 Update File And Encrypt File



Update File

File Id

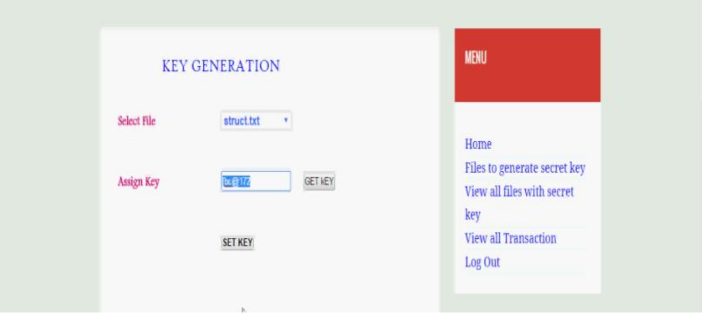
File Name

File: revocability for cloud storage system. Our system allows a sender to send an encrypted message to a receiver through a cloud storage server.

uimDY/ZBMgIo/tA6MPdB62zDgkkF9xdbX
3DckEEw6rpgfZunJB6Khmid8iekwDz1KX
EaSPAS129dyKguyUPQJezUfVWg0gFtJD4
oyp/24Top5jlxsuZZbU3aeYg7icOP0VHo
TKXqnyLurbAGg1kPtAzfAvzwUaeQF+EtS

c2Y8jmabw7GGJnBgJYOPvg%3d%3d

Figure.6 Key Generation

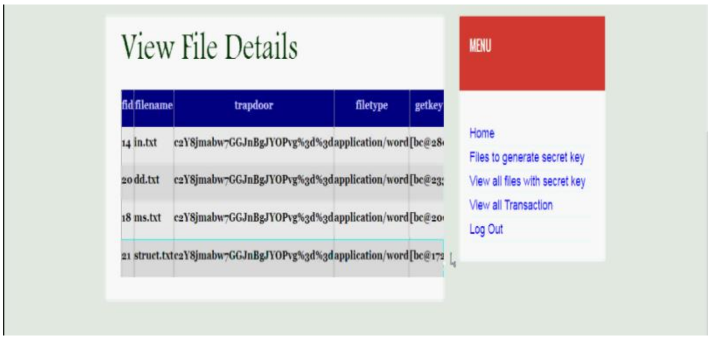


KEY GENERATION

Select File: struct.txt

Assign Key: bc@172

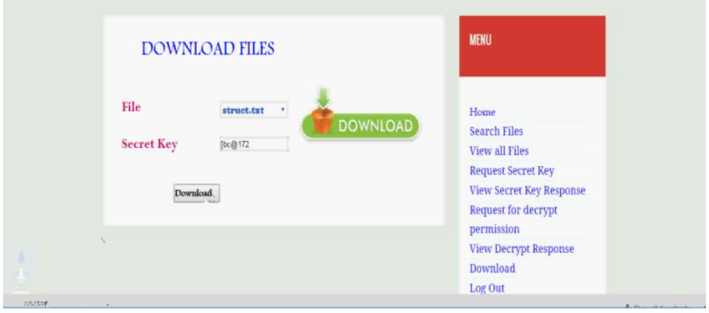
Figure.7 All Files With Secrete Key



View File Details

fid	filename	trapdoor	filetype	getkey
14	in.txt	c2Y8jmabw7GGJnBgJYOPvg%3d%3d	application/word	[bc@28
20	dd.txt	c2Y8jmabw7GGJnBgJYOPvg%3d%3d	application/word	[bc@23
18	ms.txt	c2Y8jmabw7GGJnBgJYOPvg%3d%3d	application/word	[bc@20
21	struct.txt	c2Y8jmabw7GGJnBgJYOPvg%3d%3d	application/word	[bc@172

Figure.8 Downloading the files



DOWNLOAD FILES

File: struct.txt

Secret Key: [bc@172

5. CONCLUSION

A development of computing resource professional services for both untrusted and externalised storage is proposed here. It also offered an efficient method for regular testing auditing; lowering the computing costs of the

TPA and storage network providers. The results have shown that novelty in the auditing approach has a low, consistent overhead, lowering computing and communication costs.

References

1. P. Mell and T. Grance, “Draft NIST working definition of cloud computing,” Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index. html, 2009.
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, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.
3. M. Arrington, “Gmail disaster: Reports of mass email deletions,” Online at http://www.techcrunch.com2006/12/28/gmail-disasterreports-of-mass-email-deletions/, December 2006.
4. Kincaid, “MediaMax/TheLinkup Closes Its Doors,” Online at http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/, July 2008.
5. Amazon.com, “Amazon s3 availability event: July 20, 2008,” Online at http://status.aws.amazon.com/s3-20080720.html, 2008.
6. S. Wilson, “Appengine outage,” Online at http://www.cio-weblog.com/50226711/appengine outage.php, June 2008.
7. B. Krebs, “Payment Processor Breach May Be Largest Ever,” Online at http://voices.washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.
8. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. of CCS’07, Alexandria, VA, October 2007, pp. 598–609.
9. M. A. Shah, R. Swaminathan, and M. Baker, “Privacy protection audit and extraction of digital contents,” Cryptology ePrint Archive, Report 2008/186, 2008.
10. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in Proc. of ESORICS’09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.
    A. Juels and J. Burton S. Kaliski, “Pors: Proofs of retrievability for large files,” in Proc. of CCS’07, Alexandria, VA, October 2007, pp. 584–597.
11. Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing,” 2009, http://www.cloudsecurityalliance.org.
12. H. Shacham and B. Waters, “Compact proofs of retrievability,” in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.
13. Yan Zhu, Huaixi Wang, Zexing Hu, Gail-JoonAhn,Hongxin Hu, Stephen S. Yau. "Dynamic audit servicesfor integrity verification of outsourced storages in clouds",Proceedings of the 2011 ACM Symposium on AppliedComputing - SAC '11, 2011
14. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, “Auditing to keep online storage services honest,” in Proc.Of HotOS’07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.
15. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained access control in cloud computing,” in Proc. of IEEE INFOCOM’10, San Diego, CA, USA, March 2010.
16. D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” J. Cryptology, vol. 17, no. 4, pp. 297–319, 2004.
    A. L. Ferrara, M. Greeny, S. Hohenberger, and M. Pedersen, “Practical short signature batch verification,” in Proceedings of CT-RSA, volume 5473 of LNCS. Springer-Verlag, 2009, pp. 309– 324.
17. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proc. Of SecureComm’08, 2008, pp. 1–10.
18. C.Wang, Q.Wang, K. Ren, andW.Lou, “Ensuring data storage security in cloud computing,” in Proc. of IWQoS’09, July 2009, pp. 1–9.
19. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” in Proc. of CCS’09, 2009, pp. 213–222.
20. R. C.Merkle, “Protocols for public key cryptosystems,” in Proc of IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, 1980.
21. G. Ateniese, S. Kamara, and J. Katz, “Proofs of storage from homomorphic identification protocols,” in ASIACRYPT, 2009, pp. 319–333.
22. M. Bellare and G. Neven, “Multi-signatures in the plain public key model and a general forking lemma,” in ACM Conference on Computer and Communications Security, 2006, pp. 390–399.
23. Y. Dodis, S. P. Vadhan, and D. Wichs, “Proofs of retrievability via hardness amplification,” in TCC, 2009, pp. 109–127.

24. Asraf Yasmin, B., Latha, R., & Manikandan, R. (2019). Implementation of Affective Knowledge for any Geo Location Based on Emotional Intelligence using GPS. International Journal of Innovative Technology and Exploring Engineering, 8(11S), 764–769. https://doi.org/10.35940/ijitee.k1134.09811s19
25. Muruganantham Ponnusamy, Dr. A. Senthilkumar, & Dr.R.Manikandan. (2021). Detection of Selfish Nodes Through Reputation Model In Mobile Adhoc Network - MANET. Turkish Journal of Computer and Mathematics Education, 12(9), 2404–2410. https://turcomat.org/index.php/turkbilmat/article/view/3720