International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 4, Special Issue 3 (March '2018)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

PROFICIENT PUBLIC SUBSTANTIATION OF DATA VERACITY FOR CLOUD STORAGE THROUGH DUAL PROTECTION

Prema A,
Assistant Professor,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

R.Kavitha Priyadharshini,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

N S Durga,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

J Induja,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Abstract: The cloud prosperity is one of the basic characters in cloud, here we would reservation have the capacity to our data into dispersed capacity. A consistently expanding number of clients might need to store their data to PCS (open cloud servers) nearby the quick progression of dispersed registering. Disseminated stockpiling workplaces empower customers to allocate their data to cloud servers to secure neighborhood data amassing costs. Various check errands from different customers can be performed beneficially by the evaluator and the cloud-set away data can be invigorated dynamically. It impacts the clients to check whether their outsourced data is kept set up without downloading the whole data. In our structure we are using the have examining in perspective of the token age. Using this key age methodology take a gander at the key regards from one of a kind key we can find the movements about the record. Novel open affirmations contrive for circulated capacity using as a piece of perceptibility indefinite quality, which requires a lightweight computation on the analyst and delegate most count to the cloud. Not simply set away also the substance will be encoded in the cloud server. If anyone endeavor to hack at the cloud end isn't possible to break the two particular pieces. The security of our arrangement under the most grounded security show. They require first decipher the records and moreover combine the spitted reports from three exceptional regions. This isn't possible by anyone. Anybody can download the intelligences after the waiter with best owner agreement. At the period of download key created (code based key age) and it will send to the archive proprietor. We can download the record need to use the key for check and some extraordinary customers need to download report proprietor approval is crucial.

Keywords:Cloud storage, public audit, Data integrity, Third Party Auditor (TPA) Data privacy preserving.

I.INTRODUCTION

Disseminated figuring has been envisioned as the accompanying creation information advancement (IT) building for endeavors, in view of its extended once-over of unparalleled purposes of enthusiasm for the IT history: on-ask for self-advantage, unavoidable framework get to, zone self-choosing resource pooling, snappy resource adaptability, utilize based assessing and transference of peril. As an annoying advancement with huge consequences, dispersed figuring is changing the general concept of how associations use information development. One fundamental piece of this standpoint changing is that data are being united or outsourced to the cloud. From customers' view, including together individuals and IT tries, securing data remotely to the cloud in a versatile on-ask for strategy bring charming favorable circumstancesmitigation of the weight for limit organization, boundless data access with position flexibility, and revolution of advantages use on hardware, programming, and staff frameworks for upkeeps, thus forth.While circulated figuring make these compensation more captivating than some other time in late memory, the like manner brings new and testing security risks toward customers' outsourced data. Since cloud authority centres (CSP) are part administrative components, data outsourcing is truly surrendering customer's last control more than the predetermination of their data. First of all, despite the way that the establishments under the cloud are essentially more successful and unsurprising than solitary figuring contraptions, they are up 'til now standing up to the wide extent of both inside and external risks for data genuineness. As brisk structures and general Internet find the opportunity to twist up clearly open beginning late, various associations are given on the Internet with a definite target that client can utilize them from wherever at whatever point. Information soundness is a basic requirement for restrain structures. There have been different proposition of securing information over. As a troublesome development with critical implications, circulated processing is changing the general thought of how associations use information advancement. One fundamental aspect of this perspective changing is that information are being joined together or outsourced to the cloud. From customers' perspective, including the two individuals and IT wanders, securing data remotely to the

cloud in a versatile on-ask for way brings drawing in favourable circumstances: easing of the weight for limit organization, far reaching data access with zone flexibility, and evading of capital use on apparatus, programming, and work force structures of assistance, hence forth. Cloud master associations (CSP) are separate administrative components; data outsourcing is truly surrendering customer's complete control over the fate of their data.

Appropriately, the exactness of the data in the cloud is being placed in risk as a result of the going with reasons. Above all, in spite of the way that the structures under the cloud are impressively more proficient and strong than individualized registering devices, they are up 'til now going up against the wide extent of both inside and external threats for data respectability.

II.RELATED WORKS

1. Y. Cui, Z. Lai, X. Wang, N. Dai, and C. Miao in 2015. Fast Sync: Improving Synchronization Efficiency for Mobile Cloud Storage Services As a fundamental limit of circulated stockpiling organizations, data synchronization (coordinate) engages the client to normally invigorate neighborhood record changes to the remote cloud through framework correspondences. Versatile appropriated stockpiling organizations have expanded astounding accomplishment in late couple of years. In this paper, we perceive. For example, a minor document modifying process in Drop box may realize coordinate action 10 times that of the change. Synchronization efficiency is controlled by the speed of invigorating the distinction in client records to the cloud, and considered as a champion among the most basic execution estimations for disseminated capacity organizations. We moreover complete Quick Sync to assist the modify operation with Drop box and Sea file. Our wide evaluations demonstrate that Quick Sync can feasibly save the synchronize time and diminishing the basic movement overhead for specialist coordinate workloads.

2. H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. Shen in 2014.Enabling Fine-Grained Multi-Keyword Search Supporting Classified Sub-Dictionaries Over Encrypted Cloud Data. Using conveyed processing, individuals can store their data on remote servers and allow data access to open customers through the cloud servers. As. This, in any case, by and large limits the accommodation of outsourced data in light of the inconvenience of investigating the mixed data. In this paper, we address this issue by working up the fine-grained multi-watchword look plots over encoded cloud data. Our one of a kind duties are three-overlay. In any case, we display the centrality scores and slant factors upon watchwords which engage the correct catchphrase look for and tweaked customer experience. Essentially scrambling the data may regardless reason other security concerns. For instance, Google Search uses SSL (Secure Sockets Layer) to scramble the relationship between look customer and Google server when private data, for instance, records and messages how up in the ordered records. We have explored on the fine-grained multikeyword look for (FMS) issue over mixed cloud data, and proposed two FMS designs. The FMS I fuse both the centrality scores and the slant components of catchphrases to overhaul more correct request and better customers' seeing, independently. The FMS II fulfills secure and viable interest with convenient handiness, i.e., "AND", "OR" and "NO" operations of catchphrases.

3. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li in 2013. Empowering Public Audit ability and Data Dynamics for Storage Security in Cloud Computing Distributed figuring has been envisioned as the bleeding edge plan of IT Enterprise. This work considers the issue of ensuring the trustworthiness of data accumulating in Cloud Computing. In specific, we reflect the job of letting a exile assessor (TPA), in bright of a genuine anxiety for the mist client, to checkered the decency of the lively figures usual absent in the cloud. The introduction of TPA slaughters the commitment of the client through the investigating of whether his data set away in the cloud are in actuality set up, which can be basic in finishing economies of scale for Cloud Computing. Yet envisioned as a promising organization arrange for the Internet, this new data amassing perspective in "Cloud" accomplishes many testing design issues which have critical impact on the security and execution of the general system. One of the best stresses with cloud data accumulating is that of data genuineness check at untrusted servers. Despite the way that designs. Then, to a free outcast analyst (TPA), without responsibility of their figuring resources, the clients could select the evaluation of the organization's execution. In the cloud, the clients themselves are faulty or will undoubtedly be not able hold up under the cost of the overhead of performing unending trustworthiness checks.

4. M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, and A. Y. Zomaya in 2014. Remote Data Auditing in Cloud Computing Environments: A Survey, Taxonomy, And Open Issues Treatment of Big Data and appropriated registering are the two fundamental prime concerns which have ended up being progressively standard of late. In this paper, we Distributed File System is a client based application which enables its customers to access, process and change the data which is secured on a remote server as if it existed on their neighborhood structures. Concentrated store organization is an instrument which by and large upgrades the Query response time of the record system. It empowers customers to demonstrate approaches to be saved in basic memory by HDFS. In this, the Name Node will talk with its Data Nodes that have examined the progression of dispersed record structures, their source, distinguishing strength and their change. We started our talk with the examination of Network File structure and Andrew File System. We have moreover inspected the point by point plans of GFS and HDFS, the two most significant coursed record structures of their chance adequately talented to manage the Big Data Management. A relative report between both GFS and HDFS has been done which has realized the occasion of a couple of comparable qualities and furthermore differentiates between both GFS and HDFS.

5. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song in 2015 Provable Data Possession At Untrusted Stores. Of late, appropriated processing has well-ordered transformed into the standard of Internet organizations. Right when circulated figuring circumstances end up being more perfect, the business and customer will be a monster measure of data set away However, when the data is shielded in the appropriated stockpiling contraption, a long

time, endeavors and customers certainly will have security concerns, expecting that the information is truly impregnable in the cloud is still in the limit device or too long without access to, has for quite a while been the cloud server removed or demolished. In like manner, this arrangement goal to research and framework for data storing appropriated registering circumstances that are illustrated. In this way, how to fortification data reports in the customer not the circumstance, found a capable and securely strategies for good information to perform sometimes affirmation, empowering customers to know his information record is secured securely on the server,. From the over, the customer data records set away on the server in the cloud, with a particular true objective to know whether the server truly securing data reports, customers will be perfect made to the server different troubles (Challenge), so the server that the use of the accounts were secured in the cloud does to the customer ease. Exhibits the essential customer data records set away on the server, shows the server support data to the customer truly set away on the server. In the compilation, proposed a data accumulating exhibited Provable Data Possession (PDP) system, which applies to the cloud in an suspicious amassing server, in perspective of RSA of essential plant with state affirm that the name is used to check the genuineness of the data set away in the cloud, which licenses vast number of limit server affirmation, and moreover gives an open confirmation methodology, yet also the usage of digressed key structure and the data must be determined in each piece of encoding and names the movement, making it a for the most part substantial measure of count. Stood out from the written work of PDP tradition, the composition for the past system proposed by PDP expansion of another dynamic accumulating advancement, in light of the way that, in this new technique vocations.

6. H. Lii, D. Liu, Y. Dai, and T. H. Luaan in 2012. Building Searchable Encoding Of Mobile Cloud Networks: When Qoe Meets Qop.The flexible conveyed processing applications, data outsourcing, for instance, iCloud, is basic, which outsources a versatile customer's data to outside cloud servers and fittingly gives a versatile and "constantly on" approach for open data get to. Inside resentment of the way that encryption extends the idea of confirmation (QoP) of data outsourcing, it basically reduces data accommodation and in this way harms the adaptable customer's tendency of experience (QoE).Mobile applications, for instance, relational connection, social protection, and media spilling, have quite recently transformed into an imperative bit of our step by step lives. In any case, feeble getting ready rate, and limited close-by accumulating, have out and out blocked the difference in versatile organization utilities. This article inquires about the QoE and QoP changing of data outsourcing by working up a versatile and fine-grained open encryption scheme over outsourced data. In whatever remains of this article we initially diagram the open encryption strategy in convenient cloud frameworks from the perspective of structure definition and illustrating. By then we perceive the key affecting components of QoE and QoP in open encryption and the best in class investigate.

7. Kan Yaang, Xia ohuja Jia in 2010. An Efficient and Secure Dynamic Survey Protocol in Cloud Computing for Data Storage. In aspect of the data outsourcing, regardless, this new perspective of data encouraging organization in like manner introduces new security challenges, which requires a free appraising organization to check the data rectitude in the cloud. It guarantees the data insurance against the evaluator by combining the cryptography technique with the bi-linearity property of bilinear paring, rather than using the cover framework. In this way, our multi-cloud bunch looking at tradition does not require any additional facilitator. Our bunch assessing tradition can in like manner support the group auditing for various proprietors. Furthermore, in this paper, we at first layout and analyze the structure for disseminated capacity systems and propose a beneficial and security sparing investigating tradition. By then, we extend our checking on tradition to help the data dynamic operations, which is powerful and provably secure in the sporadic prophet illustrate. We also extend our looking at tradition to help pack assessing for both diverse proprietors and different fogs, without using any place stock in organizer. The examination and entertainment occurs show that our proposed assessing traditions are secure and capable, especially it diminish the count cost of the examiner.

8. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou in 2013. Protection Preserving Public Auditing For Data Storage Security In Cloud Computing. In this paper, we utilize and uncommonly join individuals by and large key based homomorphic authenticator with sporadic veiling to fulfill the security defending open cloud data looking at structure, which meets each above essential, we furthermore research the technique of bilinear aggregate stamp to extend our essential result into a multi-customer setting, where TPA can play out various reviewing errands in the meantime. In this paper, we propose an assurance shielding open auditing system for data amassing security in Cloud Computing. We utilize the homomorphism authenticator and unpredictable disguising to guarantee that TPA would not take in any data about the data content set away on the cloud server in the midst of the compelling assessing process,. Considering TPA may all the while manage different audit sessions from different customers for their outsourced data records, we furthermore expand our assurance sparing open assessing tradition into a multi-customer setting, where TPA can play out the various looking at errands in a cluster way.

9. Giuseppe Ateniese, Roberto Di Pietro, Luigi V. Mancini, and Gene Tsudik in 2010. Adaptable and Efficient Provable Data Possession. The rule issue is the as well as frequently as could be expected under the circumstances, the limit server is believed to be untrusted to the extent both security and steadfast quality. (All things considered, it might harmfully or by chance erase encouraged data; it might moreover commit it to direct or separated accumulating.) The issue is exacerbated by the client being a bit of enrolling contraption with limited resources. In this paper, we build up an exceedingly capable and provably secure PDP technique develop absolutely in light of symmetric key cryptography, while not requiring any mass encryption. We made and showed a very much requested blueprint of a light-weight and provably secure PDP scheme. It outflanks prior work on a couple of counts, including limit, information exchange limit and figuring overheads and furthermore the assistance for dynamic operations. Regardless, since it relies upon symmetric key cryptography, it is unacceptable for open (pariah) affirmation. A trademark respond in due order regarding this would be a hybrid contrive

uniting parts of and our arrangement. To layout, the work portrayed in this paper addresses a basic progress forward towards sensible PDP frameworks. We expect that the striking features of our arrangement make it charming for sensible applications.

10. Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters in 2012Concealing Secrets In Software: A Cryptographic Approach To Program Obfuscation. In this article, we delineate some careful cryptographic reactions to these semi philosophical requests. We moreover discuss our present "rival absence of definition perplexity" plan and its recommendations. In any case, it is a rehashing subject in security outlining that insurance from one game plan of ambushes is no accreditation that a structure can't be broken by various means. Hence a substantial number of these lacks of definition designs have been trailed by looking at plans for deobfuscation. We delineated a contender absence of definition disarray design, and a segment of the invigorating applications it makes possible.

III. SYSTEM DESIGN

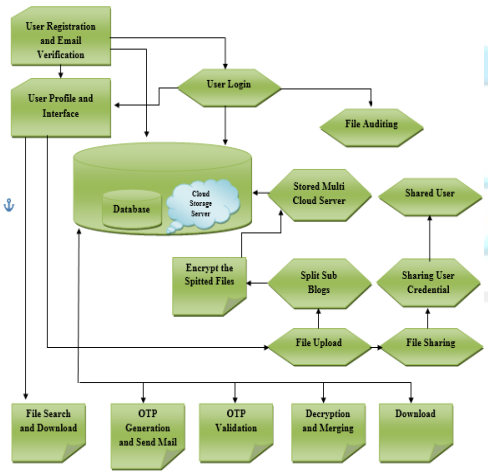

Fig 1. System deign

IV. OUR CONTRIBUTION

A. User interface:

In our Secure System we have a user friendly user interface to interact with our System. Every Act dual role as a data owner and data consumer while uploading file they are the owner of that file if they search other's file than they are the consumer. Users can create the account them self for that we have new pages, in that page we will get the details from the user and we generate the account for the user's. We have authentication system; we only allow authorized users to access our System.In our System we providing the easy file searching user's don't want to keep remember all uploaded file's exact name, for that we have given the keywords while uploading the files it will help to search the file easily.

B. File uploading process:

Storing data over storage servers one way to provide data robustness is to replicate a message such that each storage server stores a message. Another way is to encode a message of k symbols into a code word of n symbols by erasure coding. To store a message, each of its code word symbols is stored in a different storage server. A storage server corresponds to an erasure error of the code word symbol. As long as the number of servers is under the tolerance threshold of the erasure code, the message can be recovered from the code word symbols stored in the available storage servers by the decoding process.

C. Secret key generation:

Firstly the secret key will be generated as the initial step while uploading the file, every which is uploaded, will have unique secret key. This key will be taken as an identification of every file. The secret key which we are using is a three digit number we will make it use for both uploading and downloading. If the user want download some file and if he gives the download request the secret key of that file will be sent to the file owner of the file maybe he can share it.

D. File Sharing:

In our application we can share a file to a registered user by providing basic credentials, with the sharing option it is necessary to provide authority to the shared user whether to view or edit the file. A user can view the shared file within the application without downloading it and the same is possible with the edit option.

E. File Auditing:

Auditing is the process of checking the file whether the original contents of the file is changed. This module provides the file owner auditing, this we achieve by generating tokens. The tokens are generated with the ASCII values of the characters in the file and these characters are stored in the DB while uploading the file. If a shared user edit's the file and saves it, again a new token will be generated and stored in the DB. If the initial token and the current token aren't same then a notification will be sent to the file owner.

F. Mail alert process:

The uploading and downloading process of the user is first get the secret key in the corresponding user email id and then apply the secret key to encrypted data to send the server storage and decrypts it by using his secret key to download the corresponding data file in the server storage system's the secret key conversion using the Share Key Gen (SKA, t, m). This algorithm shares the secret key SKA of a user to a set of key servers.

G. File Downloading process:

File downloading process is to get the corresponding secret key to the corresponding file to the user mail id and then decrypt the file data. The file downloading process re-encryption key to storage servers such that storage servers perform the re-encryption Operation. The length of forwarded message and the computation of re-encryption is taken care of by storage servers. Proxy re-encryption Schemes significantly reduce the overhead of the data Forwarding function in a secure storage system.

V.ALGORITHMS

A. secure erasure coding

1. Begin;
2. →ow and pwd;
3. Based: = the privileges based on the entry system in the cloud computing
4. ownname =ow&& pwd=password
5. Then
6. → If(skey==cfile)
7. Files upload i;
8. i→sp1,sp2,sp3;
9. →Encryption & decryption with AES
   r→encsp1, encsp2, encsp3
   w→decsp1, decsp2, decsp3
10. file downloading fd;
11. serfile from db & server
12. if(fd==serfile)
13. Skey→send to user mail(otp).
    Add ori→(sp1+sp2+sp3)
    download the file.
    ori;
    Else
    Cancel the file;
14. End;

B. Advanced Encryption Standard (Aes)

- AES is an iterative to a specific degree than feistily figure. It depends on 'substitution– stage arrange'. It contains a progression of associated tasks, some of which include supplanting contributions by particular yields (substitutions) and others possess rearranging bits around (changes).
- AES play out all its calculation on bytes instead of bits. Henceforth, AES treats the 128 bits of a plaintext obstruct the same as 16 bytes. These 16 bytes are organized in four segments and four columns for preparing as a lattice

THE FEATURES OF AES: –

1. Symmetric key symmetric block cipher
2. 128-bit data, 128/192/256-bit keys
3. Stronger and faster than Triple-DES

Field	Type	Comment
fowner	varchar(50) NULL	
euser	varchar(50) NULL	
edfile	varchar(50) NULL	
esplit1	varchar(50) NULL	
esplit2	varchar(50) NULL	
esplit3	varchar(50) NULL	
etoken1	varchar(100) NULL	
etoken2	varchar(100) NULL	
etoken3	varchar(100) NULL	

Fig 2. Edited file

Field	Type	Comment
owner	varchar(50) NULL	
suser	varchar(50) NULL	
filenm	varchar(50) NULL	
fview	varchar(10) NULL	
fedit	varchar(10) NULL	
fdownload	varchar(10) NULL	

Fig 3. file auditing

Field	Type	Comment
name	varchar(40) NULL	
split1	varchar(500) NULL	
split2	varchar(500) NULL	
split3	varchar(500) NULL	
token1	varchar(75) NULL	
token2	varchar(75) NULL	
token3	varchar(75) NULL	
filename	varchar(500) NOT NULL	
secretkey	varchar(100) NULL	
Orfilocation	varchar(500) NULL	
counter	varchar(50) NULL	
shareduser	varchar(5000) NULL	
sival	int(5) NULL	

Fig 3 file upload

VI. CONCLUSION

A protection safeguarding open inspecting framework for information stockpiling security in processing. We use the homomorphism straight authenticator and irregular veiling to ensure that the outside asset would not take in any learning about the information content put away on the server amid the productive examining process, which not just takes out the weight of client from the dull and potentially costly inspecting errand, yet additionally mitigates the users dread of their outsourced information spillage. Considering TPA may simultaneously deal with numerous review sessions from various clients for their outsourced information documents, we additionally expand our protection saving open evaluating convention into a multiuser setting, where the TPA can play out different examining undertakings in a cluster way for better productivity.Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

VII.REFERENCES

[1]. Y. Cui, Z. Lai, X. Wang, N. Dai, and C. Miao, "Quicksync: Improving synchronization efficiency for mobile cloud storage services," in Proceedings of MobiCom. ACM, 2015, pp. 592–603.

[2]. H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325, 2016.

[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

Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.

[4]. M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, and A. Y. Zomaya, "Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues," ACM Computing Surveys, vol. 47, no. 4, 2015.

[5]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of CCS. ACM, 2007, pp. 598–609.

[6]. H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: When qoe meets qop," IEEE Wireless Communications, vol. 22, no. 4, pp. 74–80, 2015.

[7]. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013.

[8]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proceedings of INFOCOM. IEEE, 2010, pp. 1–9.

[9]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of SecureComm. ACM, 2008.

[10]. S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters, "Hiding secrets in software: A cryptographic approach to program obfuscation," Communications of The ACM, vol. 59, no. 5, pp. 113–120, 2016.

[11]. B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving PublicAuditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf.Cloud Computing, pp. 295-302, 2012.

[12]. 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.

[13]. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[14]. D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[15]. 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.

[16]. B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[17]. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[18]. The MD5 Message-Digest Algorithm (RFC1321). https://tools. ietf.org/html/rfc1321, 2014.

[19]. 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.

[20]. 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.

[21]. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.

[22]. Q. Wang, C. Wang, J. Li, K. Ren, 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.

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

[24]. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.