Journal of Engineering and Applied Sciences 13 (13): 5019-5026, 2018
ISSN: 1816-949X

Secure Big Data Storage in Cloud and Data Computing Using Cryptographic Techniques

[1]N. Madhusudhana Reddy, [2]C. Nagaraju and [3]A. Ananda Rao
[1]Department of CSE, Jawaharlal Nehru Technological University Anantapur (JNTUA), Andhra Pradesh (AP), India
[2]YSR Engineering College, Yogi Vemana University, Proddatur, Andhra Pradesh (AP), India
[3]Department of CSE Director of Academic and Planning, JNT University Ananatapur, Andhra Pradesh (AP), India

Abstract: Executing dispersed figuring empowers different routes for web-based organization offerings to address varying issues. Regardless, the data protection and assurance has transformed into a fundamental concern which limits numerous cloud submissions. One of the critical stresses in safety and assurance occurs by which that cloud executives have the possibility to accomplish and change the fragile data. This stress definitely extends customer's concern and abatements the acceptance of circulated processing in numerous fields, for instance, the money related business and regulatory associations. This study mainly concentrates on this problem and suggests an astute cryptographic technique where the cloud advantage admin can't particularly accomplish fragile data and meta cloud data storage Architecture for securing big data in cloud computing environment. The suggested approach partitions the record and freely inserts available dataset in the passed on cloud storage servers. An option is suggested to choose if the data groups require a split remembering the true objective to curtail the operation time. The suggested contrive Protection-Aware Efficient Distributed Storage (SA-EDS) illustrate which is essentially sustained by our suggested Secure Efficient Data Distributions (SED2) calculation. Our trial assessments have evaluated both safety and viability displays and the trial occurs represent that our approach can enough shield crucial dangers from fogs and requires with an suitable calculation instance.

Key words: Protection, cloud computing, delicate information, big data, distributed storage, calculation

INTRODUCTION

Dispersed figuring can portrayed as five properties, for instance, massive scalability, multi-inhabitance (shared resources), flexibility, pay only for used and self-provisioning of benefits (Purushothaman and Abburu, 2012; Schwarz and Miller, 2006). Dispersed registering enables customer to get to the remote servers encouraged on the web to store and process the data. Organization reproductions of cloud is orchestrated into 3 sorts (Wang *et al*., 2009a, b, 2012) for instance, SaaS, PaaS, IaaS and particular sending sculpts are requested into private, public and hybrid. On account of the elevated openness of the cloud to all customers, appropriated figuring goes up against more noteworthy protection challenges (Murugesan and Sudheendran, 2013). These question are accumulated into two general classes as assurance issues confronted by cloud suppliers and protection issues confronted by customers.

As one of the tremendous progressions used as a piece of circulated processing, the passed on collection has engaged (Ma *et al*., 2012; Bowers *et al*., 2009) the mass remote data aggregation by methods for Storage-as-a-Service (SaaS) advantage illustrate. This cloud advantage show has completely transformed into a tasteful approach in tremendous data nearby the progression of web organizations and frameworks (Garg and Sharma, 2013; Zhou and Huang, 2012). Many cloud shippers have given engaging gathering organization offerings that give creature and versatile cloud-dependant storage locations for customers (Vijay and Reddy, 2013; Hendricks *et al*., 2007). In any case, the protection issues occured by the procedures on cloud region is so far a block of using SaaS for wanders. Many cloud customers stress over the sensitive data where the cloud heads have the passage (Gampala *et al*., 2012). This issue mortifies existing use of SaaS in spite of the way that various prior investigates have watched out for this field.

Corresponding Author: N. Madhusudhana Reddy, Department of CSE, RGM College of Engineering and Technology, Nandyal, Andhra Pradesh (AP), India

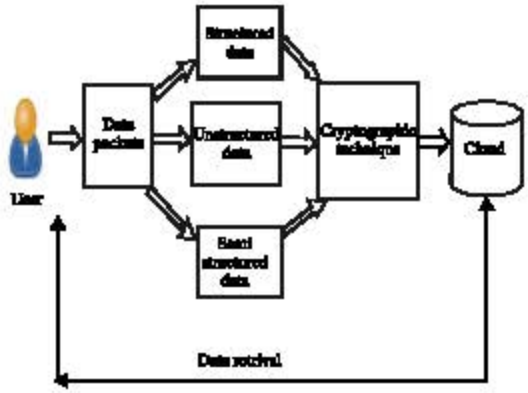

Fig. 1: Architecture of secure data storage in cloud

Additionally, Mass Distributed Storage (MDS) has investigated to increase the data aggregation measure starting late. The anomalous state presentations of the adaptable calculation are considered points of interest of completing MDS (Donald *et al*., 2013a, b; Wang *et al*., 2009a, b). One point that necessities changes is to secure circled data collection in which the dangers begin from an arrangement of sides.

This research article contemplates on the issue of cloud executives misuse issues and efforts to keep away from cloud customer's data retrieved from cloud servers. The information is considered as organized, unstructured (Guha and Shrivastav, 2013; Donald *et al*., 2013a, b) or semi-organized information in which they are put away in the cloud. We recommend an insightful cryptographic measure, named Protection-Aware Efficient Distributed Storage (SA-EDS) exhibit that is planned to get a viable MDS advantage and furthermore strange state protection confirmations. Figure 1 delineates the working of SA-EDS (Wang *et al*., 2009a, b). As showed up in Fig. 1, customer's data are reviewed by an different technique in which open named-data packs frameworks are associated. This framework is essentially kept up by our suggested calculation. In addition, part information process is refined by the focal estimation, Secure Efficient Data Distributions (SED2) Algorithm which is intended to divide information recalling a definitive goal to shield precarious data from spilling on the cloud region utilizing scarcest expenses (Ma *et al*., 2012; Ateniese *et al*., 2007).

The delicate data recuperation needs an unscrambling methodology that is reinforced by our suggested calculation. The tremendousness of the suggested part as we give an flexible approach to manage those endeavors that intend to use SaaS (Raju *et al*., 2011), however, require an anomalous state data collection protection, for instance, the cash related organization industry. The guideline issue unwound by our suggested plot is keeping cloud supplier from direct accomplishing customer's one of a kind data (Garg and Sharma, 2013; Shah *et al*., 2007). The essential duties of this article are twofold: We propose a narrative cryptographic technique for passing on mass scattered amassing by which customer's one of a kind data can't be direct come to by cloud heads. The recommended technique is a valuable cryptographic surmises for protecting destructive exercises happened on the cloud server. We propose a convincing information split part that does not pass on immense overheads (Purushotham an and Abburu, 2012; Bowers *et al*., 2009) and similarly guarantees information retrievability.

Literature review: Zhou and Huang (2012) planned to ensure data responsibility for duplicates over the flowed amassing structure. They completed the PDP plan to hide different impersonations without performing encoding on each of duplicate liberally, giving accreditation that various copies of data are truly kept up. As of late, Garg and Sharm (2013) gave an examination on many existing courses of action on isolated data trustworthiness inspecting and argued their points of interest and hindrances under diverse blueprint circumstances of protected disseminated stockpiling organizations.

Singh *et al*. (2012) proposed the provably-protected arrangement to affirm the trustworthiness of data amassing in the cloud without downloading each one of the data. The producers utilized the RSA-based homomorphic Verifiable Tag (HVT) to convey a solitary tag by joining the piece marks. HVT besides engages a server to produce a verification and empowers the customer to verify about server limitations, despite the way that the customer won't not approach the pieces. Regardless, this process gets high server caluculations or correspondence costs for the entire record on account of the usage of RSA numbering.

Shimpi *et al*. executed another kind of RDA methodology Proofs Of Accessibility (POA) to favor data respectability and to thwart data degradation with forward screw up modifying codes, remotely. The evaluator by then subjectively embeds the protected data blocks into pieces already trading towards the server. Regardless, the measure of demand in this framework is obligated to the measure of sentinel squares. The POA procedure acknowledged high calculational overhead on customer part which worked out as intended in perspective of playing out the blunder recuperation and information encryption shapes.

Ateniese *et al.* (2007) familiar a system with give adequacy and protection to the POR strategy in light of the BLS homomorphic confirmation method. The BLS technique empowers the evaluator to add up to the names into a settled size remembering the true objective to restrict the framework computational overhead, also, utilizes the Reed-Solomon policy to recoup the misunderstandings. Supporting dynamic information fortify satisfactorily is a crucial issue in most by far of the remote information evaluating systems in which the controller can intensely revive the outsourced data without recovering the outsourced record.

Wang *et al.* (2012) proposed a rank-dependent information to diagram a totally capable evaluating process. This procedure can also verify the uprightness of data squares of varied-sizes, yet, it can't affirm the reliability of individual piece. Most POR systems can't gainfully support dynamic data revive in light of the way that the server can't develop an association between the data squares and the mixed code-words.

The other weight of this method is that it can't adequately reinforce visit dynamic invigorate operations profitably due to the center point re-modifying issue and this will similarly realize elevated computational transparency on the analyst side. Additionally, bilinear coordinating calculation is more exorbitant than the logarithmic configuration which is used as a piece of our technique. The data inserted into the cloud is categorized as type 1 which is structured data and type 2 which is considered as semi-structured and unstructured data (Murugesan and Sudheendran, 2013). Here, two algorithms are used for performing encryption on both the types of data.

Algorithm 1; Types of data:

```
Selection of data (type)
If (type = = 1)
{
Structured data
Data from SQL type data bases
AESEncrypt()
Send to Cloud
}
If (type = = 2 or type = = 3)
{
Unstructured or semi structured data
Data from Hbase or Casandra or MongDB. etc
HomomorphicEncrypt()
}
```

Among the two types of data sets considered a encryption method is used to encrypt the data and then it will be stored in the cloud.

Algorithm 2; AES encryption:

```
AESEnceryption ()
{
Infer the arrangement of round keys form the figure key
Introduce the state exhibit with the piece information
(plaintext)
Add the underlying round key to the beginning stste
cluster
Perform nine rounds of state control
Duplicate the last state exhibit out as the scrambled
information (ciphertext)
}
```

The AESEncrypt() method is used for only for organized information and after that the information will be safely put away in the cloud and it is dodged from misuse (Gampala *et al*., 2012). If the information is utilized by any unapproved client then it must be decoded for understanding the information which can be done only by the authorized (Juels and Kaliski, 2007) person if the private key is provided.

Algorithm 3; Privacy key:

```
HomomorphicEncrypt ()
{
Infer the arrangement of round keys form
the figure key
Introduce the stste exhibit eith the square
information (plaintext)
Add the underlying round key to the
beginning stste cluster
Perform nine rounds of state control
Play out the tenth and last round of state
control
Duplicate the last stats cluster out as the
encoded information (ciphertext)
Step 1: Select any two prime numbers say p
and q
Step 2: compute the result of those two
prime numbers
Say N = p
classified and Nis open.
Step 3: select arbitrary number X and a root
g of GF (p). Where g and X are littler then p
Step 4: compute y = gx mod p. utilize this y
for the encryption
Step 5: encryption will be performed in
following two stages:
1. Select arbitrary whole number r and apply
following homomorphic encryption
E1 (M) = (M+r*p) mod N
2. Select arbitrary whole number k and
the encryption calculations are:
Eg (M) = (a, b) = (gk mod p, yk E1 (M) mod
p)
Step 6: Decrypted calculation Dg() is M = b×
(hatchet)- 1 (mod p)
}
```

The HomomorphicEncrypt() method is used for both semi and un structured data for performing encryption method and then it will be stored in cloud (Vijay and Reddy, 2013). The data which is encrypted with either of the methods are strongly secured from usage of data by unauthorized users.

MATERIALS AND METHODS

Secure storing of data into cloud: In cloud information collection structure, clients accumulate their information in cloud and never again have the information nearby. Thusly, the precision and transparency of the information records being secured on the scattered cloud servers must be ensured. The considerable issue is to adequately see any unapproved information adjustment and defilement, possibly as a result of server exchange off and also sporadic Byzantine disillusionments. Also, in the passed on circumstance at the point while such irregularities are effectively perceived, to determine the information held by server go of keeps in will be in like way of stunning criticalness, since, it can be the fundamental walk to quick recoup the cutoff messes up. To address these issues, our rule anticipate guaranteeing cloud information conglomeration is presented in this fragment.

The underlying fragment of a region is focused on a assessment of basic gadgets from convention speculation that is required in our arrangement for record spread transversely finished cloud servers.

Limit system design based on cloud computing: Appropriated figuring virtualization development is used as a piece of the layout of limit system to finish high synchronization and high adjustment to interior disappointment under the condition of the consistency (Donald *et al*., 2013a, b; Bowers *et al*., 2009). The pro slave dispersal configuration is used as a piece of the diagram of data amassing to keep up a vital separation from the data hardship and damage caused by the power outage under the traditional aggregation development which grasps a lone strategy for limit structure. System uses allotted limit in different physical and support gathering contraption (Wang *et al*., 2010, 2012). So, as to improve the protection and genuineness of data. Virtualized physical resources are facilitated into the pro center as the system organization center which is accountable for the organization and checking the step by step operation of the slave centers and notwithstanding ensure the run of the mill state of center points.

The expert center point sort out virtualization and flowed organization are progressed as the diagram thought to deal with the issues of pro center point organization bottleneck of the standard advancement. The pro center point is gone to by the lead recently visit, to a particular degree, relieve the passageway and organization of the pro center point inconvenience, keep up a vital separation from server disillusionments caused by consolidated access to the pro center which will incite

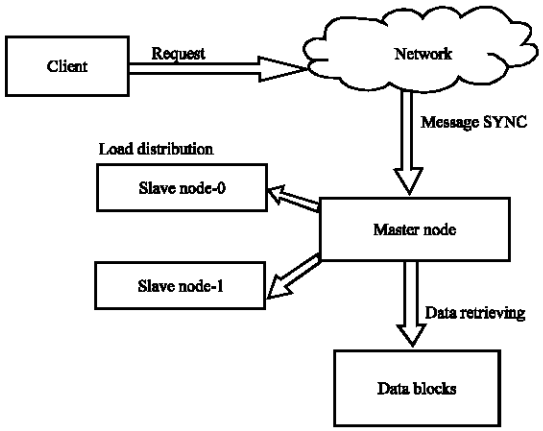

Fig. 2: Data storage method

the fold of whole system and furthermore to deal with the issue of the bottleneck of the whole structure operation, consequently improve the general capability. Various slave centers as the data amassing, finishes stack balanced scattering of set away data. The inconvenience of limit of different data sorts under the standard social database is handled and various of support amassing of data is spread into data center points (Raju *et al*., 2011; Ma *et al*., 2012). The loss of data is avoided on the begin of common system operation execution, the limit creation arrangement is showed up in Fig. 2.

Limit structure get the opportunity to stream begins with get the opportunity to request sent by client by then the message gets the chance to close expert center server through framework (Purushothaman and Abburu, 2012). After got and responded to customers request to examine and create, the center point will discover snippet of data in demonstrated slave center as showed by the convey to execute decided operation. Data is secured by allocate limit, accommodating in organization. With the usage of examination of discernment gadgets (Vijay and Reddy, 2013; Wang *et al*., 2012), electronic report is made in the customer's terminal illustrate which gives comfort in examination and decision. For whatever period of time that interfacing with the Internet client terminal can get to the structure. The terminal can be hardware, settled and mobile phones and introduced contraptions.

The steps involved in inserting the data into cloud environment is clearly explained in Fig. 2 in which based on client request the data is encoded using master node and ten it will be divided as data blocks and t hen stored in the cloud.

Protection-Alert Efficient Disseminated Storage (PA-EDS) illustrate: Our suggested SA-EDS show for the most part contains two sections, to be particular

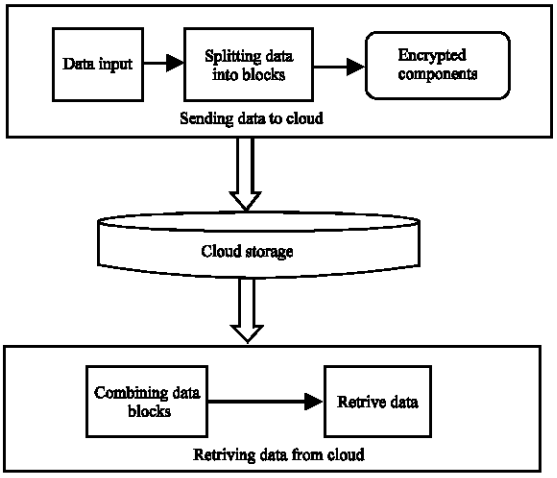

Fig. 3: Process of data stored and retrieved from cloud

Deterministic Process (DP) and Data Distributed Storage Process (D2SP). The imperative segment is intended to pick if the information bundles request an abnormal state assurance ensure. The other part is utilized to shield information from the unforeseen exercises occured by cloud-side workers. It is an inside piece of our recommended represent.

Data Disseminated Storage Process (D2SP): Figure 3 addresses an irregular state work process configuration of D2SP in the suggested SA-EDS illustrate. The recommended Fig. 3 addresses the standard plan of our point of view. The two sorts of information shape two essential strategies amidst the information transmissions.

Besides, at the accessing data available from cloud segment information clients need to get information bundles from either of cloud suppliers. Achieving the first information requires a progression of methods subsequent to the information parcels are gotten from cloud sides. In the first place, the cor-reacting information bundles should be binded up to create the new information series. Later, clients will utilize the way to do two activities took after by the underneath arrange, XOR methods to the information string and include the Key information esteem after. The first information will be increased after this method is done.

Unsafe methodologies: The cloud server generally speaking accept a confidential part in cloud advantage sending methods with the ultimate objective that many cloud advantage show planners expect that the overseers on the cloud-part are protected. Be that as it may, many threats are caused by the sudden be-haviors made by cloud administrators as opposed to the pernicious assaults. Much of the time, it transforms into a profound quality issue rather than a specialized issue, since cloud workers more often than not require the entrance to the information with the end goal of the information administration despite the fact that the exercises are limited by the directions. Then information are not secure in spite of the fact that encryptions are dependent. The data can be discharged in an extraordinary possibility if the malignant procedures are considered.

Plan goals: Our suggested framework plans to all the while accomplish a couple of focused exhibitions as takes after which can ensure the information protection required by specific information clients, for example, monetary specialists or inspecting experts: Keeping dangers from inside dangers: we hope to fulfill a bigger sum insurance data aggregation part information into different cloud servers with interior dangers can neither misuse the data nor recoup the information from the set away data into server. Data confirmation beside exterior dangers: The recommended scheme will shield data from the strikes concerned by the outside enemies. Data ought to be mixed in the midst of the conduction methodology. High viability data taking care of: Our structure will similarly keep up a key separation from high correspondence and calculation overhead remembering the true objective to drop down the torpidity. The succeeding segment portrays the principle algorithms utilized as a part of our suggested demonstrate.

Secure Efficient Data Divisions (SED2) algorithm: SED2 algorithm is intended to achieve the information handling previous tramission to cloud space. The yields incorporate two separate encoded information α and β. Executing SED2 calculation can skillfully shield the hazard models. In ARCT hazard illustrate, acknowledge that cloud delegates have the key and can access to the data on the server. Deficient data don't contain any information while the most important data won't be gained until the point that two areas are cooperated. Furthermore in MAT hazard illustrate, the foes have foundation data about the information and mean to mishandle the information. In this manner, our suggested plan can adequately shield both risk models in the hypothetical point of view. Simulated codes of SED2 is represented in Algorithm 4 and 5.

Algorithm 4; Codes of SED2:

Algorithm: Secure Efficient Data Distributions (SED2)algorithm.
Requri: D, C
Ensure: α, β
1: Input D, C
2: Initialize R← 0, α← 0, β← 0
3: /*C is a random binary that is shorter than D*/
4: Randomly generate a key K

5: for ∀ input data packets do
6: if D = = C&&C = = 0 then
7: DO R← D← C
8: α← C_ K
9: β← R_ K
10: endif
11: end for
12: Output α, β

The main steps of Algonrithm are given as follows:

Algorithm 5; SED2:

1. Input data packet D and C. Data C needs to be a non-empty set that is shorter than D. C should not be as same as D. Create and initialize a few data set, R, α and β; assign 0 value to each of them
2. Randomly generate a key K that is stored at the User's special register for the pupose of encryption and decryption. This is the crucial part for protecting privacy before the data sre sent out
3. We calculate the value of R by (D-C), then execute two XOR operations to obtain the data value stored in the clouds. The data in the renote storage are denoted to α and β. We use the following formulas to obtain α and β: α = C_ K; β = R_K
4. Output α and βand sparately story them in the different cloud servers

RESULTS AND DISCUSSION

This area demonstrateed a few test happens made in our execution evaluations. Figure 4 and 5 laid out an examination of the completing point among EDS and AES. We utilized the same measured information and dismembered the encrypted point in time employments. Figure 4 and 5displayed several outcomes that were made under setting 1-1 and 1-2. As exhibited by the lines appeared in Fig 4 and 5, our recommended plot had a shorter execution time than AES under both demonstrated situations. The unraveling time necessary is more broadened day and age under the two settings.

The number of iterations leves performed on the data sets for providing protection with encryption methodologies is clearly depicted in Fig. 4 which compares the levels with existing system.

The importance of the use of data for the wander is explored in this paper in the underlying stride. To satisfy the demand of huge data taking care of stage, data application arrange in Hadoop and data blend organize in data stockroom are progressed. Disseminated processing advancement is grasped in the arrangement of limit

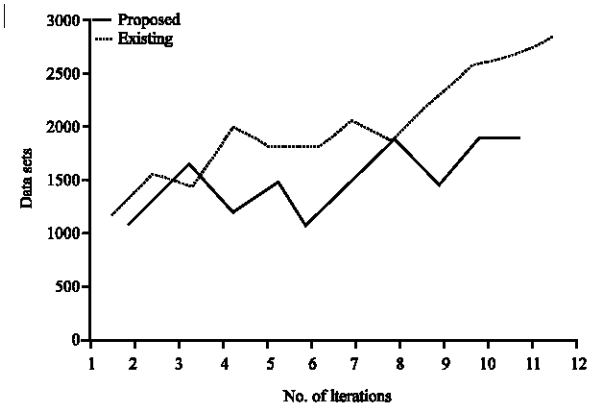

Fig. 4: Iteration level comparison with existing and suggested algorithms

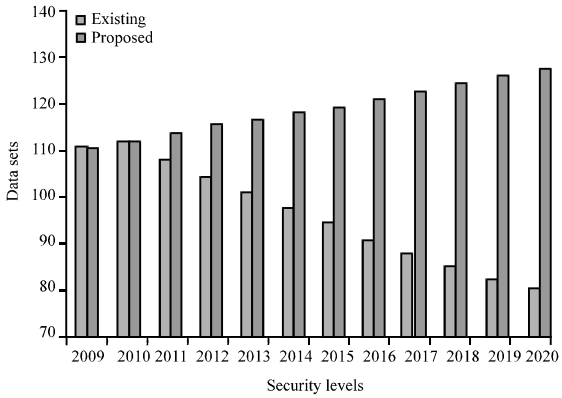

Fig. 5: Protection levels in existing and suggested systems

structure and advances the standard development in the expert center point server organization in coursed limit by contrasting the protection levels are shown in Fig. 5. Through separating and recognizing key developments of limit structure, for instance, archive square invigorate framework and accuse recovery instruments, achievable particular game plans away organization for colossal data are given.

CONCLUSION

In this study, we look at the issue of data protection in cloud data gathering which is fundamentally an appropriated aggregation structure. To finish the affirmations of cloud data respectability and openness and maintain the idea of reliable dispersed stockpiling advantage for customers, we propose a fruitful and versatile passed on contrive with unequivocal dynamic data reinforce including square revive, delete and include. By utilizing the time, calculation resources and associated

online weight of customers, we also give the continuation of the suggested guideline intend to help third party assessing where customers can safely choose the uprightness checking endeavors to outcast evaluators and be easy to use the circulated stockpiling organizations. Through distinct protection and expansive examination comes to fruition, we exhibit that our arrangement is exceedingly viable and solid to Byzantine dissatisfaction, toxic data change strike and altogether server plotting attacks.

SUGGESTIONS

In this study, we suggested meta cloud data storage architecture for securing big data in cloud computing environment. Guide reduce structure is used to find the amount of customers who were marked into the cloud server cultivate. Suggested framework guarantees the mapping of various data segments to each provider using meta cloud data storage interface. Despite the way this suggested approach requires high use effort, it gives critical information to circulated processing condition that can have high impact on the bleeding edge structures. Our future research is to grow the suggested meta cloud data storage architecture for steady planning of spouting data.

REFERENCES

Ateniese, G., R. Burns, R. Curtmola, J. Herring and L. Kissner *et al*., 2007. Provable data possession at untrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security, October 28-31, 2007, ACM, Whistler, Canada, ISBN:978-1-59593-703-2, pp: 598-609.

Bowers, K.D., A. Juels and A. Oprea, 2009. HAIL: A high-availability and integrity layer for cloud storage. Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'09), November 09-13, 2009, ACM, Chicago, Illinois, ISBN:978-1-60558-894-0, pp: 187-198.

Donald, A.C., S.A. Oli and L. Arockiam, 2013. Mobile cloud protection issue and challenge: A perspective. Intl. J. Eng. Innovative Technol., 3: 401-406.

Donald, A.C., S.A. Oli and L. Arockiam, 2013. Mobile cloud security issues and challenges: A perspective. Intl. J. Electron. Inf. Technol., 3: 1-6.

Gampala, V., S. Inuganti and S. Muppidi, 2012. Data security in cloud computing with elliptic curve cryptography. Intl. J. Soft Comput. Eng., 2: 138-141.

Garg, P. and V. Sharma, 2013. Secure data storage in mobile cloud computing. Intl. J. Sci. Eng. Res., 4: 1154-1159.

Guha, V. and M. Shrivastava, 2013. Review of information authentication in mobile cloud over SaaS and PaaS layers. Intl. J. Adv. Comput. Res., 3: 116-121.

Hendricks, J., G.R. Ganger and M.K. Reiter, 2007. Verifying distributed erasure-coded data. Proceedings of the 26th Annual ACM Symposium on Principles of Distributed Computing, August 12-15, 2007, ACM, Portland, Oregon, ISBN:978-1-59593-616-5, pp: 139-146.

Juels, A. and B.S.Jr. Kaliski, 2007. PORs: Proofs of retrievability for large files. Proceedings of the 14th ACM Conference on Computer and Communications Security, October 29-November 2, 2007, ACM, New York, USA., ISBN:978-1-59593-703-2, pp: 584-597.

Ma, L., J. Sum and Y. Li, 2012. Comparing general paradigm on data secrecy protection for outsourced file in mobile cloud computing. J. Netw., 7: 1449-1455.

Murugesan, K. and S. Sudheendran, 2013. Ensuring user security and data integrity in multi-cloud. Intl. J. Soft Comput. Eng., 3: 355-358.

Purushothaman, D. and S. Abburu, 2012. An approach for data storage security in cloud computing. Intl. J. Comput. Sci. Issues, 9: 100-105.

Raju, V., R. Kumar and A. Raj, 2011. Techniques for efficiently ensuring data storage security in cloud computing. Intl. J. Comp. Tech. Appl., 2: 1717-1721.

Schwarz, T.S. and E.L. Miller, 2006. Store, forget and check: Using algebraic signatures to check remotely administered storage. Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06), July 4-7, 2006, IEEE, Lisboa, Portugal, pp: 12-12.

Shah, M.A., M. Baker, J.C. Mogul and R. Swaminathan, 2007. Auditing to keep online storage services honest. Proceedings of the 11th USENIX Workshop on Hot Topics in Operating Systems, May 7-9, 2007, USENIX Association, Berkeley, California, USA., pp: 1-6.

Singh, K., I. Kharbanda and N. Kaur, 2012. Protection issue occurs in cloud computing and their solution. Intl. J. Comput. Sci. Eng., 4: 945-949.

Vijay, G.R. and A.R.M. Reddy, 2013. Data protection in cloud based on trusted computing environment. Intl. J. Soft Comput. Eng., 3: 187-191.

Wang, C., Q. Wang, K. Ren and W. Lou, 2010. Privacy-preserving public auditing for data storage security in cloud computing. Proceedings of the 2010 IEEE Conference on INFOCOM, March 14-19, 2010, IEEE, San Diego, California, pp: 1-9.

Wang, C., Q. Wang, K. Ren and W. Lou, 2009a. Ensuring data storage security in cloud computing. Proceedings of the 2009 17th International Workshop on Quality of Service IWQoS09, July 13-15, 2009, IEEE, Charleston, South Carolina, USA., ISBN:978-1-4244-3875-4, pp: 1-9.

Wang, C., Q. Wang, K. Ren, N. Cao and W. Lou, 2012. Toward secure and dependable storage services in cloud computing. IEEE. Trans. Serv. Comput., 5: 220-232.

Wang, Q., C. Wang, J. Li, K. Ren and W. Lou, 2009b. Enabling public verifiability and data dynamics for storage security in cloud computing. In: Computer Security-ESORICS 2009, Backes, M. and P. Ning (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-04443-4, pp: 355-370.

Zhou, Z. and D. Huang, 2012. Efficient and secure data storage operations for mobile cloud computing. Proceedings of the 8th International Conference on Network and Service Management (CNSM) and 2012 Workshop on Systems Virtualiztion Management (SVM), October 22-26, 2012, IEEE, Nevada, USA., ISBN:978-1-4673-3134-0, pp: 37-45.