IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 3, Ver. I (May.-June. 2017), PP 38-49
www.iosrjournals.org

Review of Key Management and Distribution Technique for Data Dynamics for Storage Security in Cloud Computing

Dharam Raj Kumar[1], Dr. Jitendra Sheetalani[2]
[1, 2](Sri Satya Sai University & Medical Sciences, Sehore, India)

Abstract: *Data storage and retrieval is major issue in cloud environments. For data storage and retrieval used authentication and authorization process. The authentication and authorization process used cryptography technique. The cryptography technique provides symmetric and asymmetric crypto systems. The symmetric technique is week in compression of asymmetric technique. Various authors used the concept of asymmetric cryptography technique for the process of data over the cloud network. Authors also suggested the concepts of data dynamics for the proof of data retrieval. The proof of retrieval gives the concept of cloud based data auditing in block level. The access of data security faced a problem of encryption time of data and generation of key. The encryption time and generation of key take more time and invites third party attack on data integration. For the integration of data various algorithms are used. In this paper present the review of key generation and crypto analysis of data over cloud computing.*

Keywords: *Cloud, Data Storage, Cryptography, RSA, Proof of Retrieval*

I. Introduction

Key generation and management of key distribution play an important role in cloud data storage. In cloud data storage, basically three parties are involved during the data retrieval and data storage. First is user, second one is TPA and third one is cloud server. The storage of data over cloud provide user authentication mode in three different segments. One form user to TPA and second one is TPA to server and third one is cloud server to user. In overall scenario, key distribution play an important role. Cloud data storage and access of data faced a big security issue in concern of security and validation of user authentication. For the authentication of user used various cloud security model. All cloud security model used cryptography technique for the generation of key for access of data and retrieval of data. The generation of key handles by server and take more time for the generation of key and access of data. Now key generation and handling of key in cloud computing is big issue. Now a day's various authors used various key distribution and key authentication technique such as AES, DSS, RSA ECA and many more technique for the grouping of key. The process of key generation take more time and invite many man and middle attack on the time of retrieval of data. Now for the minimization of time in key generation policy is big issue. There are many types of access control mechanisms in different systems, but the main idea is controlling read and write access, which fall under confidentiality, and besides that, ensuring data integrity. Finally, it is also important that the stored data is always available, but it is solely the task of the server to provide availability for the data. To sum up, we can have three levels of access permission to the stored data. To achieve a system that covers the above specifications for access control, we use cryptography. By using cryptography, we can perform the operations locally on the client, which additionally increases the security level. For data confidentiality, symmetric encryption can be used, and for data integrity, asymmetric encryption can be used. In one of the coming sections (section 3.3), we would discuss about why it would be reasonable to use both encryption mechanisms. The owner of the stored data has of course all three access permissions, because he has created all three keys, but by distributing keys as required, he can grant different access permission other users. So, this mechanism is best suited to be used in constructing the basis for the Secure Access Control system. As specified above, we know that the main difference between the specified mechanism and other available mechanisms is that here the security operations can be performed. Cloud Computing is not just a third-party data warehouse [27]. The data stored in the cloud may be frequently updated by the users, including insertion, deleting, modification, appending, reordering, etc [21][22][25][26][40]. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. Recently, the importance of ensuring the remote data integrity has been highlighted by the following research works [3] [4] [5] [6] [7]. These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage,

since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols [8] [9] [10][25][]26 for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited. In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data[28][47]. The most general form of these operations we are considering is block update, delete, insert and append. The rest of paper describe as in section II discuss related work. In section III. Discuss key generation process. In section IV discuss experimental result and finally discuss conclusion & future work in section V.

II. Related Work

In this section discuss the security of cloud storage process over the internet. The various authors are used various cryptography technique some technique discuss here. Shucheng Yu, Cong Wang, KuiRen and Wenjing Lou Et al. [1] They accomplish this objective by abusing and interestingly consolidating methods of characteristic based encryption (ABE), intermediary re-encryption, and sluggish re-encryption. their talked about plan likewise has remarkable properties of client get to benefit confidentiality and client mystery key responsibility. Broad examination demonstrates that their talked about plan is exceptionally efficient and provably secure under existing security models. This paper goes for fine-grained information get to control in distributed computing. One test in this setting is to accomplish fine-grandness, information confidentiality, and adaptability all the while, which is not given by current work. They talked about a plan to accomplish this objective by misusing KP-ABE and particularly joining it with systems of intermediary re-encryption and sluggish re-encryption. Cong Wang, Sherman S.- M. Chow, Qian Wang, Kui Ren and Wenjing Lou Et al. [2] In this paper, they talked about a protection saving open inspecting framework for information stockpiling security in Cloud Computing. they use the homomorphic straight authenticator and irregular veiling to ensure that the TPA would not take in any learning about the information content put away on the cloud server amid the efficient examining process, which not just wipes out the weight of cloud client from the dreary and potentially costly reviewing errand. Considering TPA may simultaneously deal with numerous review sessions from various clients for their outsourced information files, they additionally broaden their protection saving open evaluating convention into a multi-client setting, where the TPA can play out different inspecting undertakings in a cluster way for better efficiency. Broad examination demonstrates that their plans are provably secure and very efficient. Sherman S.M. Chow, Cheng-Kang Chu, Xinyi Huang, Jianying Zhou and Robert H. Deng Et al. [3] One worry in utilizing distributed storage is that the touchy information ought to be confidential to the servers which are outside the trust space of information proprietors. They concentrate the different elements offered by cryptographic unknown verification and encryption instruments; and instantiate their outline with verifier-neighborhood revocable gathering mark and personality based communicate encryption with steady size figure writings and private keys. To understand their idea, they outfit the communicate encryption with the dynamic figure content refresh highlight, and give formal security ensure against versatile picked figure content decoding and refresh assaults. Zhihua Xia, Xinhui Wang, Xingming Sun and Qian Wang Et al. [4] In this paper, a protected, efficient and dynamic inquiry plan is examined, which underpins the precise multi-watchword positioned seek as well as the dynamic cancellation and inclusion of reports. they develop an extraordinary watchword adjusted twofold tree as the file, and talked about a "Voracious Depth-first Search" calculation to acquire preferred efficiency over direct pursuit. Trial comes about show the efficiency of their talked about plan. There are as yet many test issues in symmetric SE plans. In the talked about plan, the information proprietor is in charge of creating refreshing data and sending them to the cloud server. In this manner, the information proprietor needs to store the decoded file tree and the data that are important to recalculate the IDF values. Such a dynamic information proprietor may not be extremely appropriate for the distributed computing model. Really, there are many secure difficulties in a multi-client plot. Firstly, every one of the clients normally keep the same secure key for trapdoor era in a symmetric SE conspire. For this situation, the denial of the client is enormous test. In the event that it is expected to renounce a client in this plan, they have to remake the record and circulate the new secure keys to all the approved clients. Furthermore, symmetric SE plots for the most part expect that every one of the information clients are dependable. It is not functional and an exploitative information client will prompt many secure issues. Cong Wang, Qian Wang, Kui Ren and Wenjing Lou Et al. [5] In this paper, they examined a protection saving open reviewing framework for information stockpiling security in Cloud Computing. They use the homomorphic authenticator and irregular covering to ensure that TPA would not take in any information about the information content put away on the cloud server amid the efficient inspecting process, which not just wipes out the weight of cloud client from the

dull and potentially costly reviewing errand, additionally mitigates the clients' dread of their outsourced information spillage. Considering TPA may simultaneously deal with numerous review sessions from various clients for their outsourced information files, they additionally broaden their protection safeguarding open inspecting convention into a multi-client setting, where TPA can play out the different evaluating errands in a group way, i.e., all the while. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou Et al. [6] In this paper, they have talked about a novel structure of secure sharing of individual wellbeing records in distributed computing. Considering in part reliable cloud servers, they contend that to completely understand the patient-driven idea, patients should have finish control of their own security through scrambling their PHR files to permit fine-grained get to. they use ABE to encode the PHR information, so patients can permit get to by individual clients, as well as different clients from open areas with various expert parts, qualifications and affiliations. Facilitate more, they upgrade a current MA-ABE plan to deal with efficient and on-request client disavowal, and demonstrate its security. Through usage and reenactment, they demonstrate that their answer is both versatile and efficient. Kan Yang and Xiaohua Jia Et al. [7] In this paper, they first plan an evaluating structure for distributed storage frameworks and talked about an efficient and protection saving reviewing convention. They talked about an efficient and characteristically secure element examining convention. It secures the information protection against the evaluator by joining the cryptography strategy with the bi-linearity property of bilinear paring, instead of utilizing the veil method. Along these lines, their multi-cloud bunch reviewing convention does not require any extra coordinator. their group inspecting convention can likewise bolster the bunch evaluating for numerous proprietors. Besides, their examining plan acquires less correspondence cost and less calculation cost of the evaluator by moving the figuring heaps of inspecting from the inspector to the server, which extraordinarily enhances the reviewing execution and can be connected to huge scale distributed storage frameworks. Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen and Athanasios V. Vasilakos Et al. [8] In this paper, The itemized examination is given to acquire an ideal testing size to limit the cost. Another real commitment of this paper is that they construct a down to earth secure-mindful distributed computing trial condition, or SecHDFS, as a proving ground to execute SecCloud. Advance test comes about have shown the viability and efficiency of the talked about SecCloud. they have defined the ideas of un-cheatable cloud calculation and protection deceiving disheartening and examined SecCloud to accomplish the security objectives. To enhance the efficiency, distinctive clients' solicitations can be simultaneously dealt with through the group verification. By the broad security examination and execution recreation in their created SecHDFS, it is demonstrated that their convention is successful and efficient for accomplishing a safe distributed computing. C. Selvakumar, G. JeevaRathanam and M. R. Sumalatha Et al. [9] In this paper the parceling technique is talked about for the information stockpiling which stays away from the neighborhood duplicate at the client side by utilizing apportioning strategy. This strategy guarantees high distributed storage uprightness, improved mistake limitation and simple recognizable proof of getting out of hand server. They examined a productive information stockpiling security in cloud benefit. The dividing of information empowers putting away of the information in simple and viable way. It likewise gives route for adaptable get to and there is less cost in information stockpiling. The space and time is additionally successfully decreased amid capacity. Dynamic operation is another key idea where, encoding and translating process secures information, when putting away into cloud. Additionally the remote information honesty checking identifies the dangers and making trouble server while putting away the information in cloud guaranteeing information security. A. Rajathi and N. Saravanan Et al. [10] Cloud stockpiling administration maintains a strategic distance from the cost costly on programming, staff support and gives better execution, less capacity cost and versatility. This work overviewed on a few existing distributed storage systems, strategies and their points of interest, downsides and furthermore talks about the difficulties that are required to execute secure cloud information stockpiling. Distributed computing is a rising figuring worldview, permits clients to share assets and data from a pool of conveyed processing as an administration over Internet. Despite the fact that Cloud gives advantages to clients, security and protection of put away information in cloud are as yet significant issues in distributed storage. Distributed storage is a great deal more gainful and invaluable than the prior conventional stockpiling frameworks particularly in adaptability, cost diminishment, conveyability and usefulness prerequisites. This paper introduced a study on secure stockpiling strategies in Cloud Computing. Initial a few stockpiling procedures that give security to information in cloud have been talked about in detail. At last, displayed a relative examination on capacity procedures, that incorporates the talked about approach, preferences and confinements of those capacity systems. C. Chris Erway, AlptekinKüpçü, CharalamposPapamanthou and Roberto Tamassia Et al. [11] they consider the issue of efficiently demonstrating the uprightness of information put away at untrusted servers. In the provable information ownership (PDP) show, the customer preprocesses the information and after that sends it to an un-confided in server for capacity, while keeping a little measure of meta-information. The customer later requests that the server demonstrate that the put away information has not been messed with or erased. They demonstrate that customers of an untrusted CVS server even those putting away none of the formed assets locally can question the server to demonstrate

ownership of the archive utilizing only a little division of the data transfer capacity required to download the whole vault. "Evidence size and time per submit" allude to a proof sent by the server to demonstrate that a solitary confer was performed effectively, speaking to the ordinary utilize case. These submit evidences are little and quick to process, rendering them reasonable despite the fact that they are required for each confer. their tests demonstrate that their DPDP plan is efficient and reasonable for use in disseminated applications. Cong Wang and Kui Ren Et al. [12] in this article they master represent that openly auditable cloud information stockpiling can help this early cloud economy turn out to be completely settled. They first present a system design for adequately portraying, creating, and assessing secure information stockpiling issues. They then propose an arrangement of deliberately and cryptographically attractive properties for open examining administrations of tried and true cloud information stockpiling security to end up distinctly a reality. Through top to bottom investigation, some current information stockpiling security building squares are inspected. The upsides and downsides of their handy ramifications with regards to distributed computing are abridged. Additionally difficult issues for open evaluating administrations that should be centered around are examined as well. they trust security in distributed computing, a region loaded with difficulties and of central significance, is still in its outset now however will pull in tremendous measures of research exertion for a long time to come. Lan Zhou, Vijay Varadharajan and Michael Hitchens Et al. [13] In this paper, they depict a down to earth usage of the talked about RBE-based engineering and examine the execution comes about. they exhibit that clients just need to keep a solitary key for decoding, and framework operations are efficient paying little respect to the many-sided quality of the part chain of command and client participation in the framework. Frst they talked about another RBE plot that accomplishes efficient client renouncement. At that point they displayed a RBAC based distributed storage engineering which permits an association to store information safely in an open cloud, while keeping up the touchy data identified with the association's structure in a private cloud. At that point they have built up a protected distributed storage framework engineering and have demonstrated that the framework has a few prevalent qualities, for example, steady size cyphertext and unscrambling key. From their tests, they watch that both encryption and unscrambling calculations are efficient on the customer side, and decoding time at the cloud can be lessened by having various processors, which is basic in a cloud situation. they trust that the talked about framework can possibly be helpful in business circumstances as it catches commonsense get to strategies in light of parts in a flexible way and gives secure information stockpiling in the cloud authorizing these get to arrangements. Kan Yang and Xiaohua Jia Et al. [14] In this paper, they defined another get to control structure for multi-specialist frameworks in distributed storage and talked about an efficient and secure multi-expert get to control plot. they first planned an efficient multi-specialist CP-ABE conspire that does not require a worldwide expert and can bolster any LSSS get to structure. At that point, they demonstrated that their multi-specialist CP-ABE plan is provably secure in the irregular prophet display. they likewise talked about another strategy to tackle the trait denial issue in multi-specialist CP-ABE frameworks. The examination and reproduction comes about demonstrated that their talked about get to control plan is versatile and efficient. Kan Yang and Xiaohua Jia Et al. [15] in this paper, they researched the reviewing issue for information stockpiling in distributed computing and examined an arrangement of prerequisites of outlining the Third-Party Auditing conventions. They likewise portrayed and broke down the current reviewing strategies in the writing. At long last, they talked about some difficult issues in the plan of proficient reviewing conventions for information stockpiling in distributed computing.

.

III. Cloud Key Management

Key management is the set of techniques involves generation, distribution, storage, and revoking, verifying keys. Key management can be applied to Cloud Infrastructure. In this section, we present the taxonomy of key management for Cloud storage based on location of placing key and describe various key management methods. Fig. describes key management taxonomy [16][17][18][29][30].

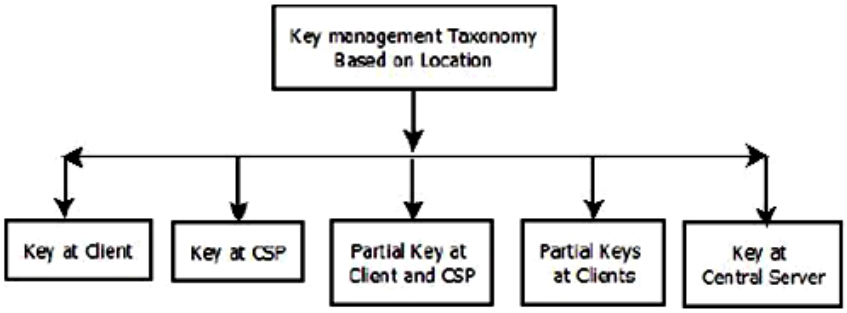

Fig.1: Shows that key taxonomy of key generation technique.

1. Management Of Key At Client Side

In this approach, data will be stored at cloud service provider side in encrypted form. Client may be thin e.g. mobile phone. Keys will be maintained at customer side. Usually this approach is taken in Homomorphism cryptographic technique. Operations are done on encrypted data at server side [8, 9]. Figure describes key management approach. In this approach, mobile phone user and desktop user maintains key at its own side [20].

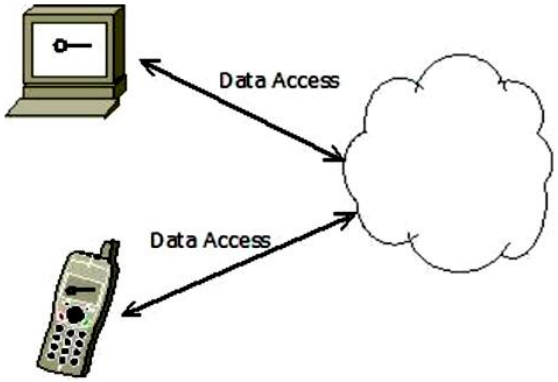

Fig.2: Keys at Client side.

2. Key Management At Cloud Service Provider Side

In this approach, keys are maintained at cloud service provider side. If the key is lost, customer is unable to read data which is present at cloud. Data is stored in the encrypted form and decrypted by the key to get it in the original form [37][38][39].

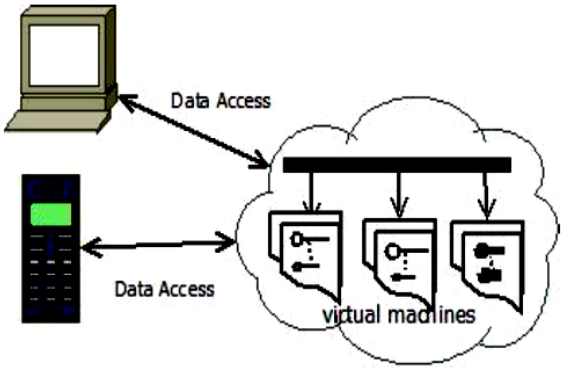

Fig.3: Shows that key maintained in cloud server side.

3. Management Of Key At Both Sides

In this technique, key is divided into two parts. One part is stored at user side and other part is stored at cloud side. If both parts are combined together, it is possible to retrieve the data properly. Thus, data remains the secure and can be controlled by the user. Thus, solution is also scalable. Cloud service provider and user do not need to maintain complete key at Cloud side. If part of the key is lost, data cannot be recovered[27][28].

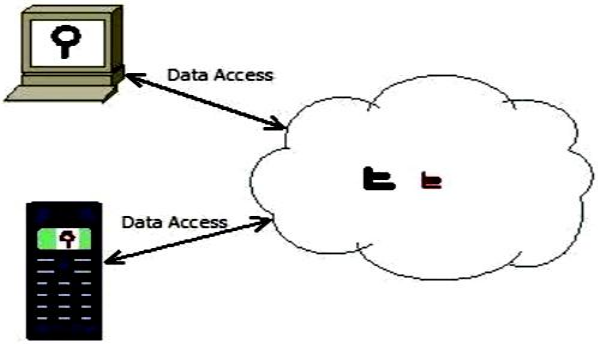

Fig.4: Shows Management of Key at Both Sides.

4. Key Splitting Technique

Content provider share data in cloud so as to accessible by the other users. Key is spitted and distributed among the users. If particular user has to access the data from the cloud, first he/she needs to get the partial keys from the users. If k out of n keys is combined, then user is able to encrypt and decrypt the data. [19][31]

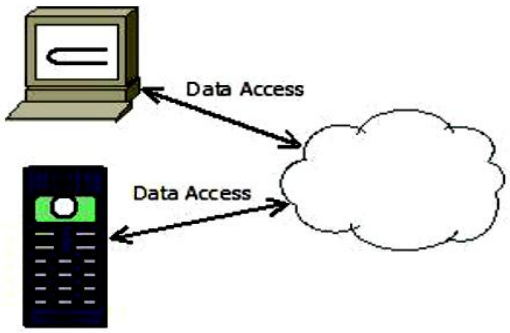

Fig.5: Shows Key Splitting Technique.

5. Key Management At Centralized Server

This approach uses asymmetric key approach. Data is encrypted with the public key stored in key server. Data at cloud side is stored in the encrypted form. The user accesses the data. This will be decrypted by private key maintained at each user. Disadvantage of this method is that if key server is crashed, its single point of failure [2, 12, 13, 32, and 39].

Fig. 6 shows that each user generates public and private keys. Public keys are stored at Key server. Suppose mobile phone user wants to share data with desktop user. He/She will encrypt the data with public key of desktop user. Thus desktop user will access data with its private key [48][49][50].

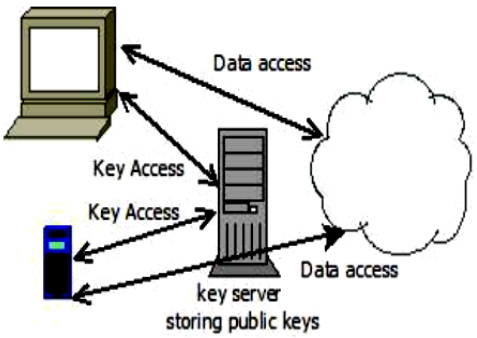

Fig.6: Shows Key Management at Centralized Server.

6. Group Key Management For Cloud Data Storage

Data is shared in cloud by trusted members of the group. Group key is established for securing data at cloud side. Group key is formed by the partial keys maintained at each user. If particular group members want to access the data, group key used to access the data. If member leaves the group, group key is formed again. If member joins the group, group key is established among members [42][44][45][46].

IV. Experimental Analysis

In this section analysis, the key generation algorithm based on key length size and data size encryption over the cloud network. The analysis of result evaluated in two scenarios one is encryption time and other is fake and genuine file during the retrieval of data from storage side. The analysis of process used two software one Is MATLAB and other is java based cloud environments [32][33][34][35].

Table 1: Shows that the comparative performance for original and fake files based on number of hit and miss ratio in percentage value for the PQR and XYZ file.

TYPES OF FILE	FILE NAME	HIT RATIO (%)	MISS RATIO (%)	DATA TYPE VALUE
ORIGINAL FILE	PQR.txt	0.9	0.1	False
FAKE FILE	XYZ.txt	0.85	0.15	True

Table 2: Shows that the comparative performance for original and fake files based on number of hit and miss ratio in percentage value for the RS and TU file.

TYPES OF FILE	FILE NAME	HIT RATIO (%)	MISS RATIO (%)	DATA TYPE VALUE
ORIGINAL FILE	RS.txt	0.88	0.12	False
FAKE FILE	TU.txt	0.81	0.19	True

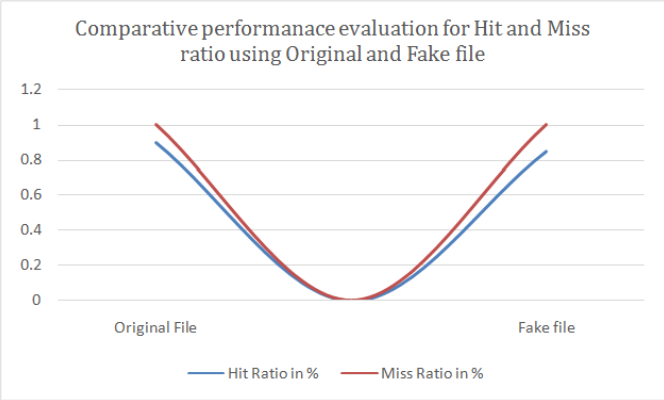

Fig.7: Shows that the comparative performance evaluation graph for original and fake files based on number of hit and miss ratio in percentage value for the PQR and XYZ file.

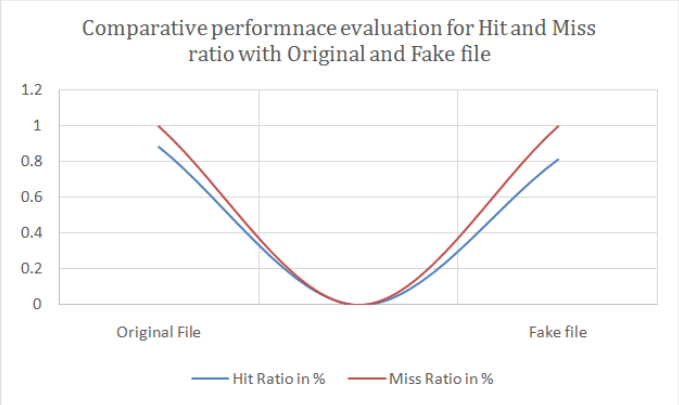

Fig.8: Shows that the comparative performance evaluation graph for original and fake files based on number of hit and miss ratio in percentage value for the RS and TU file.

Table 3: Shows that the comparative performance for Computation time on the basis of block size using methods DRDP, RSA Based and Cyclic Based.

DRDP METHOD		RSA BASED INSTANTIATION		CYCLIC BASED	
BLOCK DATA SIZE	COMPUTATION TIME	BLOCK DATA SIZE	COMPUTATION TIME	BLOCK DATA SIZE	COMPUTATION TIME
0	200	0	220	0	210
20	220	20	240	20	230
40	240	40	260	40	250
60	260	60	280	60	270
80	280	80	300	80	290
100	300	100	320	100	310
120	320	120	340	120	330
140	340	140	360	140	350
160	360	160	380	160	370
180	380	180	400	180	390

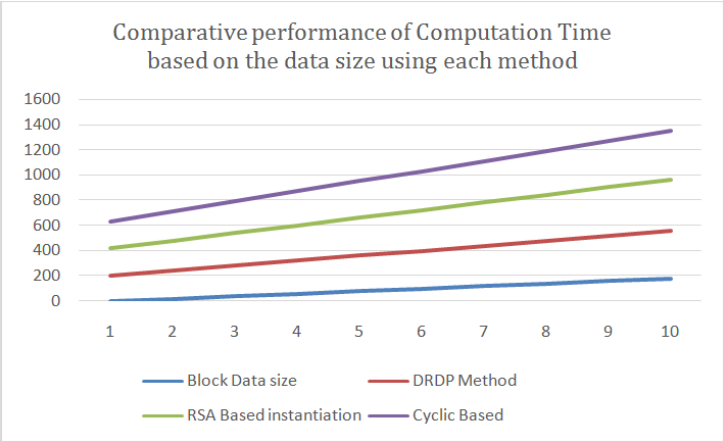

Fig.9: Shows that the comparative performance for Computation time on the basis of data block size using each method like DRDP, RSA Based and Cyclic Based, here we find the value of computation time for respectively block size and methods.

In this section, we described the various comparative performance evaluation techniques for the key management and generation in cloud computing mechanism. Here we apply the different number of keys in the form of input with different number of various key generation techniques and get the result with correspondence of each key and techniques in the form of result or output[36][41][43].

Table 4: Comparative performance evaluation using for the number of key generation techniques with the input value is 125.

INPUT KEY VALUE	NAME OF TECHNIQUES	ELAPSED TIME
125	AES	1.956
	TRIPLEDES	1.034
	BLOW FISH	8.102
	RC4	7.563

Table 5: Comparative performance evaluation using for the number of key generation techniques with the input value is 128.

INPUT KEY VALUE	NAME OF TECHNIQUES	ELAPSED TIME
128	AES	1.201
	TRIPLEDES	9.561
	BLOW FISH	8.342
	RC4	8.122

Table 6: Comparative performance evaluation using for the number of key generation techniques with the input value is 256.

INPUT KEY VALUE	NAME OF TECHNIQUES	ELAPSED TIME
256	AES	1.157
	TRIPLEDES	1.201
	BLOW FISH	7.734
	RC4	6.902

Table 7: Comparative performance evaluation using for the number of key generation techniques with the input value is 384.

INPUT KEY VALUE	NAME OF TECHNIQUES	ELAPSED TIME
384	AES	1.221
	TRIPLEDES	2.155
	BLOW FISH	8.162
	RC4	1.502

Table 8: Comparative performance evaluation using for the number of key generation techniques with the input value is 512.

INPUT KEY VALUE	NAME OF TECHNIQUES	ELAPSED TIME
512	AES	1.402
	TRIPLEDES	1.066
	BLOW FISH	1.205
	RC4	7.472

Comparative Result Graph

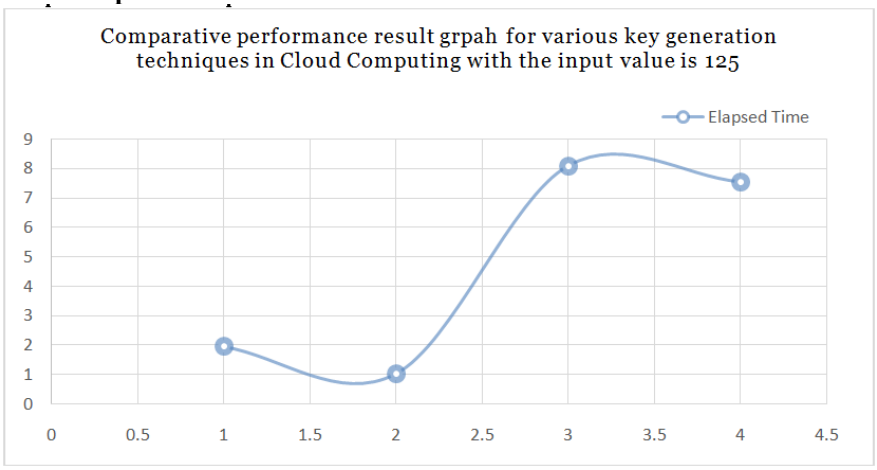

Fig.10: Figure shows that a compartive performance evaluation using different number of key genration techniques in cloud computing enviornment with the input value is 125, here we get the result in the form of Elapsed Time or Execution Time.

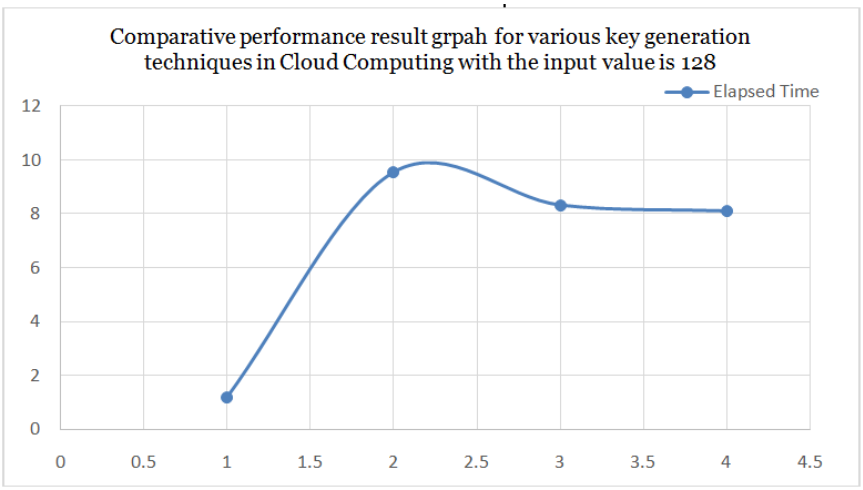

Fig.11: Figure shows that a compartive performance evaluation using different number of key genration techniques in cloud computing enviornment with the input value is 128, here we get the result in the form of Elapsed Time or Execution Time.

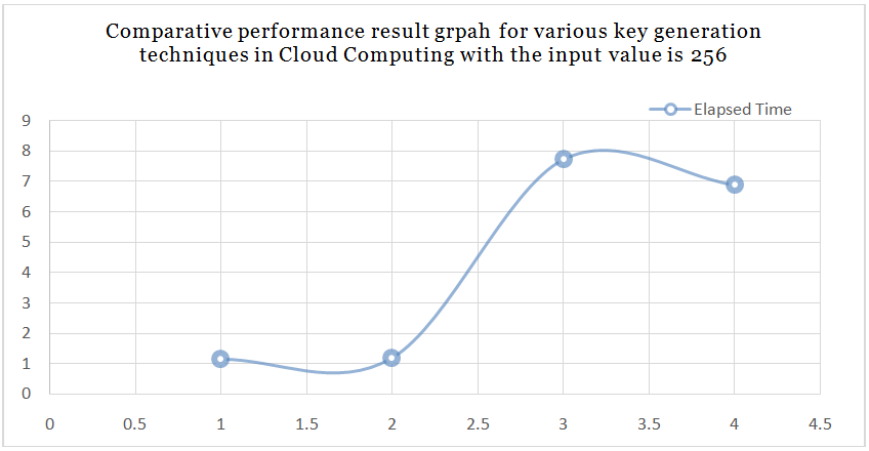

Fig.12: Figure shows that a compartive performance evaluation using different number of key genration techniques in cloud computing enviornment with the input value is 256, here we get the result in the form of Elapsed Time or Execution Time.

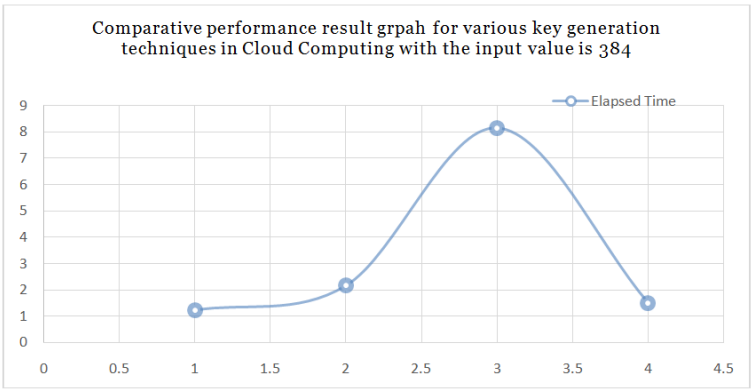

Fig.13: Figure shows that a compartive performance evaluation using different number of key genration techniques in cloud computing enviornment with the input value is 384, here we get the result in the form of Elapsed Time or Execution Time.

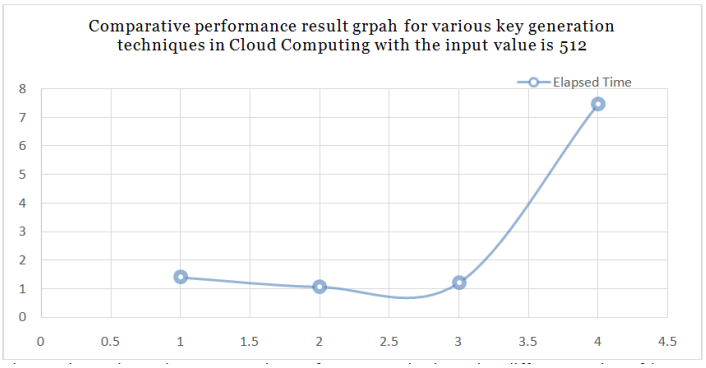

Fig.14: Figure shows that a compartive performance evaluation using different number of key genration techniques in cloud computing enviornment with the input value is 512, here we get the result in the form of Elapsed Time or Execution Time.

V. Conclusion & Future Scope

In this paper present the experimental review of key generation process in cloud data storage over the internet. In the process of experimental review found that most of authors used asymmetric key cryptography technique based on block and bit level. The size of key is increase the complexity of generation process is also increase. Instead of key generation technique also review the concept of data dynamics of different algorithm. the data dynamics process used the concept of proof of data retrieval over the internet. These responsibilities differ by the kind of cloud services been consumed. The cloud service provides is on duty to ensure the security of cloud data storage and to ensure maximum protection. Service providers have the responsibility to ensure the public data integrity and isolation protections are put in place to mitigate the risks users pose to one another in terms of data loss, misuse, or privacy violation within the cloud. Again, from the cloud service provider's perspective, there should be an active monitoring mechanism in place to allow for effective planning and implementation of services. proposed key generation demonstrates how integrity verification can be done with just transfer of few bites and offline execution of necessary algorithms. It also offers secure access control, managing access rights mechanism, audit trail, better performance and reduced overhead.

References

[1] Shucheng Yu, Cong Wang, KuiRen and Wenjing Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, IEEE, 2010, 1-9.
[2] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren and Wenjing Lou, Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE, 2013, 1-12.
[3] Sherman S.M. Chow, Cheng-Kang Chu, Xinyi Huang, Jianying Zhou and Robert H. Deng, Dynamic Secure Cloud Storage with Provenance, Springer, 2011, 442-464.
[4] Zhihua Xia, Xinhui Wang, Xingming Sun and Qian Wang, A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data, IEEE, 2015, 1-13.
[5] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, IEEE, 2010, 1-9.
[6] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption, IEEE, 2013, 1-14.

[7] Kan Yang and Xiaohua Jia, An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, IEEE, 2012, 1-11.

[8] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen and Athanasios V. Vasilakos, Security and privacy for storage and computation in cloud computing, Information Sciences, 2014, 371–386.

[9] C. Selvakumar, G. JeevaRathanam and M. R. Sumalatha, PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique, IEEE, 2012, 7-11.

[10] A. Rajathi and N. Saravanan, A Survey on Secure Storage in Cloud Computing, Indian Journal of Science and Technology, 2013, 4396-4401.

[11] C. Chris Erway, AlptekinKüpçü, CharalamposPapamanthou and Roberto Tamassia, Dynamic Provable Data Possession, ACM, 2010, 213-222.

[12] Cong Wang and Kui Ren, Toward Publicly Auditable Secure Cloud Data Storage Services, IEEE, 2010, Pp 19-24.

[13] Lan Zhou, Vijay Varadharajan and Michael Hitchens, Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage, IEEE, 2013, 1947-1960.

[14] Kan Yang and Xiaohua Jia, Attributed-based Access Control for Multi-Authority Systems in Cloud Storage, IEEE, 2012, Pp 536-545.

[15] Kan Yang and Xiaohua Jia, Data storage auditing service in cloud computing: challenges, methods and opportunities, World Wide Web, 2012, 409–428.

[16] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 2011, 1-11.

[17] Kan Yang, Xiaohua Jia and Kui Ren, Attribute-based Fine-Grained Access Control with Efficient Revocation in Cloud Storage Systems, ACM, 2013, 523-528.

[18] Chirag Modi, Dhiren Patel, Hiren Patel, BhaveshBorisaniya, Avi Patel and MuttukrishnanRajarajan, A survey of intrusion detection techniques in Cloud, Journal of Network and Computer Applications, 2013, 42-57.

[19] Yan Zhu, Huaixi Wang, Zexing Hu, Gail-JoonAhn, Hongxin Hu and Stephen S. Yau, Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds, ACM, 2013, 1550-1557.

[20] Yan Zhu, Gail-JoonAhn, Hongxin Hu, Stephen S. Yau, Ho G. An, and Shimin Chen, Dynamic Audit Services for Outsourced Storages in Clouds, IEEE, 2011, 1-14.

[21] Cong Wang, Qian Wang, Kui Ren, Ning Cao and Wenjing Lou, Towards Secure and Dependable Storage Services in Cloud Computing, IEEE, 2012, 1-14.

[22] Yongjun Ren, Jian Shen, Jin Wang, Jin Han and Sungyoung Lee, Mutual Verifiable Provable Data Auditing in Public Cloud Storage, Mutual Verifiable Provable Data Auditing in Public Cloud Storage, 2015, 317-323.

[23] Sandeep K. Sood, A combined approach to ensure data security in cloud computing, Elsevier, 2012, 1831-1838.

[24] Deepak Puthal, Surya Nepal, Rajiv Ranjan and Jinjun Chen, A Dynamic Key Length based Approach for Real-Time Security Verification of Big Sensing Data Stream, springer, 2015, 1-15.

[25] Mazhar Ali, Samee U. Khan and Athanasios V. Vasilakos, Security in cloud computing: Opportunities and challenges, Information Sciences, 2015, 357–383.

[26] Boyang Wang, Sherman S.M. Chow, Ming Li and Hui Li, Storing Shared Data on the Cloud via Security-Mediator, IEEE, 2013, 124-133.

[27] Abdul Nasir Khan, M.L. Mat Kiah., Sajjad A. Madani, Atta ur Rehman Khan and Mazhar Ali, Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing, Springer, 2013, 1-20.

[28] Kan Yang and Xiaohua Jia, Data storage auditing service in cloud computing: challenges, methods and opportunities, World Wide Web, 2012, 409–428.

[29] Lifei Wei, Haojin Zhu, Zhenfu Cao, Weiwei Jia and Athanasios V. Vasilakos, SecCloud: Bridging Secure Storage and Computation in Cloud, IEEE, 2010, 52-61.

[30] Ning Cao, Shucheng Yu, Zhenyu Yang, Wenjing Lou and Y. Thomas Hou, LT Codes-based Secure and Reliable Cloud Storage Service, IEEE, 2012, 693-701.

[31] Chirag Modi, Dhiren Patel, BhaveshBorisaniya, Avi Patel and MuttukrishnanRajarajan, A Survey on Security Issues and Solutions at Different Layers of Cloud Computing, springer, 2013, 1-31.

[32] Swapnil V. Khedkar and A. D. Gawande, Data Partitioning Technique to Improve Cloud Data Storage Security, IJCSIT, 2014, 3347-3350.

[33] Lanxiang Chen and Gongde Guo, An Efficient Remote Data Possession Checking in Cloud Storage, International Journal of Digital Content Technology and its Applications, 2011, 43-50.

[34] Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou, Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data, IEEE, 2014, 1-9.

[35] Smitha Sundareswaran, Anna Squicciarini and Dan Lin, A Brokerage-Based Approach for Cloud Service Selection, IEEE, 2012, 558-565.

[36] Sameer Pawar, Salim El Rouayheb and Kannan Ramchandran, On Secure Distributed Data Storage Under Repair Dynamics, arXiv, 2010, 1-5.

[37] Dimitrios Zissis and DimitriosLekkas, Addressing cloud computing security issues, Future Generation Computer Systems, 2012, 583–592.

[38] Hongwei Li, Yuanshun Dai and Bo Yang, Identity-Based Cryptography for Cloud Security, IACR, 2011, 1-9.

[39] T. Venkateswara Rao and V Pradeep, Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage, International Journal of Applied Sciences, Engineering and Management, 2015, 56 – 59.

[40] Zhibin Zhou and Dijiang Huang, Efficient and Secure Data Storage Operations for Mobile Cloud Computing, IFIP, 2012, 37-45.

[41] Rohit Bhadauria and SugataSanyal, Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques, arXiv, 2012, 1-20.

[42] M.Sudha and M.Monica, Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography, Advances in Computer Science and its Applications, 2012, 32-37.

[43] Piotr K. Tysowski and M. Anwarul Hasan, Re-Encryption-Based Key Management Towards Secure and Scalable Mobile Applications in Clouds, IEEE, 2013, 1-10.

[44] Lanxiang Chen, Using algebraic signatures to check data possession in cloud storage, Future Generation Computer Systems, 2013, 1709–1715.

[45] Deyan Chen and Hong Zhao, Data Security and Privacy Protection Issues in Cloud Computing, International Conference on Computer Science and Electronics Engineering, 2012, 647-651.

[46] Ming Li and Wenjing Lou, Data Security and Privacy In Wireless Body Area Networks, Wireless Technologies For E-Healthcare, 2010, 51-58.
[47] NayotPoolsappasit, RinkuDewri and Indrajit Ray, Dynamic Security Risk Management Using Bayesian Attack Graphs, IEEE, 2012, 1-17.
[48] Alejandro Russo and Andrei Sabelfeld, Dynamic vs. Static Flow-Sensitive Security Analysis, ACM, 2010, 1-21.
[49] Miao He, Junshan Zhang and Vijay Vittal, A Data Mining Framework for Online Dynamic Security Assessment: Decision Trees, Boosting, and Complexity Analysis, IEEE, 2011, 1-8.
[50] J. Aghaei, N. Amjadyb and H.A. Shayanfar, Multi-objective electricity market clearing considering dynamic security by lexicographic optimization and augmented epsilon constraint method, Applied Soft Computing, 2011, 3846–3858.