ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Key Agreement for Sharing Dynamic Data with Different Group for Re Construction Using Blocks Level

Bhavna A. Khairnar, Pravin P. Nimbalkar

M. E Student, Department of Computer Engineering, Imperial College of Engineering and Research Pune, India

Professor, Department of Computer Engineering, Imperial College of Engineering and Research Pune, India

ABSTRACT: In Cloud Computing Data Sharing empowers various members to uninhibitedly share the distinctive gathering information, which generally enhance the proficient of work in helpful. The most effective method to guarantee the security of information sharing inside gathering and redistributed information in gathering way are formable difficulties. The Key conventions have assumed a critical job in secure and productive gathering in distributed computing. To Prevent this issue in this paper, Symmetric adjusted fragmented square structure (SBIBD) are utilized for key Security and un-approved client can't get to the Data from various gathering. SBIBD is utilized the general recipe for creating the basic meetings key K for numerous Participants. General equation (v, k+1, 1) square plan is utilized to information are put away. As Result of putting away information from dynamic gathering and Data are separated Blocks and System Performances are a superior when contrasted with Exiting Scheme with help of best calculations is Blows fish and DES and Encryption utilized as completely Homomorphism encryption .

KEYWORDS: Multi cloud storage, information leakage, system attack-ability, remote synchronization, distribution and optimization.

I.INTRODUCTION

In Cloud Computing Data Sharing empowers various members to unreservedly share the diverse gathering information, which broadly enhance the proficient of work in helpful. Instructions to guarantee the security of information sharing inside gathering and redistributed information in gathering way are formable difficulties. The Key conventions have assumed an essential job in secure and effective gathering in distributed computing. To Prevent of this issue in this paper, Symmetric adjusted inadequate square structure (SBIBD) are utilized for key Security and un-approved client can't get to the Data from various gathering. SBIBD is utilized the general recipe for producing the basic meetings key K for different Participants. General recipe (v, k+1, 1) square structure is utilized to information are put away. As Result of putting away information from dynamic gathering and Data are partitioned Blocks and System Performances are a superior when contrasted with Exiting Scheme with help of best calculations is Blows fish and DES and Encryption utilized as completely Homomorphism encryption.With the increasingly rapid uptake of devices such as laptops, cellphones and tablets, users require an ubiquitous and massive network storage to handle their ever-growing digital lives. To meet these demands, manycloud-based storage and file sharing services such as Drop box, Google Drive and Amazon S3, have gained popularity due to the easy-to-use interface and low storage cost. However, these centralized cloud storage services are criticized for grabbing the control of users' data, which allows storage providers to run analytics for marketing and advertising . Also, the information in users' data can be leaked e.g., by means of malicious insiders, backdoors, bribe and coercion. One possible solution to reduce the risk of information leakage is to employ multi cloud storage systems in which no single point of attack can leak all the information. A malicious entity, such as the one revealed in recent attacks on privacy , would be required to coerce all the different CSPs on which a

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

user might place her data, in order to get a complete picture of her data. Put simply, as the saying goes, do not put all the eggs in one basket.

Cloud computing and cloud storage have become hot topics in recent decades. Both are changing the way we live and greatly improving production efficiency in some areas. At present, due to limited storage resources and the requirement for convenient access, we prefer to store all types of data in cloud servers, which is also a good option for companies and organizations to avoid the overhead of deploying and maintaining equipment when data are stored locally. Recently, the development of cloud computing boosted some applications where the cloud service is used as a collaboration platform. In these software development environments, multiple users in a group need to share the source code, and they need to access, modify, compile and run the shared source code at any time and place. The new cooperation network model in cloud makes the remote data auditing schemes become infeasible, where only the data owner can update its data. Obviously, trivially extending a scheme with an online data owner to update the data for a group is inappropriate for the data owner. It will cause tremendous communication and computation overhead to data owner, which will result in the single point of data owner. To support multiple user data operation, Wang proposed data integrity based on ring signature. In the scheme, the user revocation problem is not considered and the auditing cost is linear to the group size and data size. To further enhance the previous scheme and support group user revocation, Wang et al. designed a scheme based on proxy re-signatures. However, the scheme assumed that the private and authenticated channels exist between each pair of entities and there is no collusion among them. Also, the auditing cost of the scheme is linear to the group size.

Motivation:-

There are lots of user preference cloud Services for Data Storage but there is no Assurance for the secure data on cloud that why our system given some effective work to Cloud Server Provider for the purposed of Data Storing

1. In cloud computing consistent view of resources is not monitored which lacks the actual condition & hence in case of faults heavy data losses or data availability reduction occurs.
2. Centralized resource manager is not identified which shares the distributed load information for first level encryption admin is performance and accurate analysis is done by cloud services provider.
3. In cloud computing security is major factor of data and key related concepts so our application is used as concepts of KASE.
4. Dynamic and efficient key management for access hierarchies.
5. Simple and fault-tolerant key agreement for dynamic collaborative data of groups.

II.REVIEW OF LITERATURE

In this work [1] Y. Amir as proposed Group key agreement is a fundamental building block for secure peer group communication systems. Several group key management techniques were predictable in the last decade, all assuming the survival of an underlying group communication infrastructure to provide dependable and ordered message delivery as well as group membership information. Despite analysis, implementation, and utilization of some of these techniques, the actual costs allied with group key management have been poorly understood so far. This resulted in an uninvited tendency: on the one hand, adopting suboptimal precautions for consistent group communication, while, on the other hand, constructing excessively precious group key management protocols. In this work D. Augot, R. Bhaskar as projected A Group Key Agreement (GKA) etiquette is a mechanism to launch a cryptographic key for a group of participants, based on each one's contribution, over a public network. The key, thus derived, can be used to establish a secure channel between the participants. When the group concerto changes (or otherwise), one can utilize supplementary GKA protocols to obtain a new key. Thus, they are well-matched to the key establishment needs of self-motivated peer-to-peer networks as in ad hoc networks. While many of the future GKA protocols are too luxurious to be employed by the inhibited devices often present in ad hoc networks, others lack a formal security analysis. In this work they present a simple, sheltered and capable GKA protocol well suited to active ad hoc networks. They also

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

present results of our accomplishment of the protocol in a prototype application. Storage outsourcing is a rising trend which prompts a number of interesting security issues, many of which have been broadly investigated in the past. m.

In this work [3] A. Beimel and B. Chor as projected Social Network Services (OSNs) are today one of the most popular interactive medium for communication, sharing, and disseminating a significant amount of human subsistence information. It involves swap of several types of content, including free text, picture, audio, and video data. However, OSNs features a large number of attacks that affects the privacy and security of users. So, a new community network is considered for enabling privacy security for the OSN users by offering them to open and constructive network. Here, the author uses a group key agreement problem where a user is only aware of his neighbors while the connectivity graph is random. Key agreement is a method that allows two or more parties to firmly share a secret key.

In this work [4] R. Blom, proposed there is an ever-growing need for "trusted" devices, and as a result, assurances from technology for fiddle resistance and read-proofing of secrets stored in such devices. They converse a simple security policy - decrypt only when obligatory (DOW N) - and its inference on the security of secrets stored in trusted computers. The DOW N policy used in combination with the budding paradigm of physical unlovable functions (PUF) can be a hopeful approach for recognition of trusted computers. A simple security policy, DOWN, can considerably improve the ability of trusted computers to protect their secrets. The emerging paradigm of physical un-closable functions (PUF) [3], used in concurrence with the DOWN policy, can further improve trustworthiness of computers. .

In this work [5] D. Boneh and M. K. Franklin has proposed that Data storage is now an important development inclination in information technology. However, information security has become an important problem to hamper it for commercial application, such as data discretion, integrity, and accessibility. In this paper, we propose elected verifier provable data possession (DV-PDP). In public clouds, DV-PDP is a matter of critical importance when the client cannot execute the remote data possession checking. They study the DV-PDP system security model and utilize Encased homomorphism m authenticator to design DV-PDP scheme. The scheme detached exclusive bilinear computing. Moreover in DV-PDP scheme, the Data storage Data Server is stateless and independent from verifier, which is an vital secure property in PDP schemes. Through security study and recital analysis, our scheme is demonstrable secure and high competence.

In this work [6] D. Boneh, C. Gentry, and B. Waters Provable data possession (PDP) is a performance for ensuring the truthfulness of data in storage outsourcing. In this paper, the author address the construction of an efficient PDP scheme for distributed Data storage to support the scalability of service and data migration, in which they consider the continuation of multiple Data service providers to cooperatively store and maintain the clients' data. cooperative PDP (CPDP) scheme based on homomorphism confirmable response and hash index hierarchy. They prove the security of our scheme based on multi-proverb zero knowledge proof system, which can satisfy completeness, knowledge soundness, and zero-knowledge properties. In addition, we coherent concert optimization mechanisms for our scheme and in meticulous present a competent method for selecting optimal parameter standards to minimize the totaling costs of clients and storage service providers. Our experiments show that our explanation introduces lower working out and communication operating expense in comparison with non-cooperative approaches. In this work

[7] D. Boneh, A. Sahai, and B. Waters Provable data possession is a procedure for ensuring the integrity of data in outsourcing storeroom service. In this paper, they propose a cooperative verifiable data possession format in hybrid clouds to bear scalability of service and data migration, in which they deem the existence of multiple Data service providers to cooperatively store up and sustain the clients' data. Our experiments demonstrate that the verification of their scheme requires a small, constant amount of overhead, which minimizes communication complication.

In this work [8] D. Boneh and M. Naor many storage systems rely on imitation to augment the availability and durability of data on untrusted storage systems. At present, such storage systems provide no strong confirmation that multiple copies of the data are actually stored. Storage Data Servers can conspire to make it look like they are storing many copies of the data, whereas in authenticity they only store a single copy. We address this shortcoming through multiple-replica attestable data possession (MR-PDP): A provably-secure scheme that allows a client that provisions replicas of a file in a storage system to authenticate through a challenge-response etiquette that each unique replica can be shaped at the time of the challenge and that the storage system uses t times the storage required to store a single replica. MRPDP extends previous work on data ownership proofs for a single copy of a file in a client/Data Server storage system. Using MR-PDP to lay up t replicas is computationally much more resourceful than using a single-

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

replica PDP format to store t separate, dissimilar files (e.g., by encrypting each file separately prior to storing it). Another benefit of MR-PDP is that it can generate further replicas on demand, at little expense, when some of the accessible replicas fail.

In this work [9] D. Boneh and A. Silverberg has planned cryptologic multi linear maps are terribly helpful in cryptography however their construction is one among the long-standing open drawback. Recently, 2 candidates of the cryptologic multi linear map are planned from plan of the somewhat holomorphic secret writing theme. During this speak, they have a tendency to review the definition of cryptologic multi linear map that starts with linear map with several attention-grabbing applications. They have a tendency to gift a summary of the planned 2 candidates for the multi linear map and compare their structures with the underlying somewhat holomorphic encryptions.

Public key encryption with keyword search We consider the issue of looking for on data that is encoded using an open key system. Consider customer Bob who sends email to customer Alice mixed under Alice's open key. An email passage needs to test whether the email contains the catchphrase "earnest" with the target that it could course the email fittingly. As another depiction, consider a mail server that stores different messages direct encoded for Alice by others. Using our instrument Alice can send the mail server a key that will engage the server to see all messages containing some express catchphrase, regardless get nothing else. We portray open key encryption with watchword request and give a few upgrades [10].

“Vabks: Verifiable attribute-based keyword search over outsourced encrypted data” Typically nowadays for data proprietors to re-appropriate their data to the cloud. Since the cloud can't be totally trusted, the re-appropriated data should be encoded. This in any case brings an extent of issues, for instance, How should a data proprietor give look capacities to the data customers? In what way can the endorsed data customers look for over a data proprietor's re-appropriated mixed data? By what means can the data customers be ensured that the cloud dependably executed the interest assignments for the wellbeing of they? Impelled by these request, we propose a novel cryptographic course of action, called evident trademark based catchphrase look (VABKS). The game plan allows a data customer, whose accreditations satisfy a data proprietor's passageway control system, to (I) investigate the data proprietor's re-appropriated encoded data, (ii) redistribute the grim interest errands to the cloud, and (iii) affirm whether the cloud has constantly executed the request exercises. We formally describe the security essentials of VABKS and portray an improvement that satisfies them. Execution appraisal exhibits that the proposed plans are reasonable and deployable [11].

Fluffy character based encryption. We present another sort of Identity-Based Encryption (IBE) plot that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we see a way of life as set of illuminating properties. A Fuzzy IBE invent thinks about a private key for a character, ω, to unravel a figure content encoded with a personality, ω 0 , if and just if the characters ω and ω 0 are near each other as assessed by the "set cover" clear measurement. A Fuzzy IBE plan can be connected with enable encryption using biometric duties as identities; the error obstruction property of a Fuzzy IBE plot is totally what considers the use of biometric characters, which ordinarily will have some clamor each time they are dismembered. In like manner, we demonstrate that Fuzzy-IBE can be utilized for a sort of utilization that we term "trademark based encryption". In this paper we indicate two headways of Fuzzy IBE plans. Our headways can be seen as an Identity-Based Encryption of a message under several properties that shape a (padded) character. Our IBE structures are both blunder tolerant and secure against intrigue ambushes. Moreover, our essential headway does not utilize sporadic prophets. We demonstrate the security of our plans under the Selective-ID security show[12]

“Searchable encryption revisited: Consistency properties, relation to anonymous IBE and extensions” We see and fill two or three openings as to consistency (how much false positives are made) for open key encryption with watchword search for (PEKS). We depict computational and authentic relaxations of the present thought of impeccable consistency, demonstrate that the game plan of is computationally constant, and give another course of action that is quantifiably trustworthy. We in like way give a distinction in a weird IBE plan to an anchored PEKS plot that, not in any way like the past one, ensures consistency. At long last we propose three improvements of the essential insights considered here, explicitly astounding HIBE, open key encryption with brief catchphrase demand, and character based encryption with watchword look [13].

“Anonymous hierarchical identity-based encryption (without random oracles)” We show a character based cryptosystem that highlights absolutely cloud figure writings and distinctive leveled key task. We give a proof of security in the standard model, in light of the fragile Decision Linear multifaceted nature supposition in bilinear social gatherings. The framework is incredible and supportive, with little figure writings of size direct in the noteworthiness of the chain of hugeness. Applications join enthusiasm on encoded information, absolutely private correspondence, and so forth. Our outcomes settle two open issues relating to darken character based encryption, our course of action being the first to offer provable puzzle in the standard model, regardless of being the first to perceive absolutely peculiar HIBE at all measurements in the chain of significance [14].

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

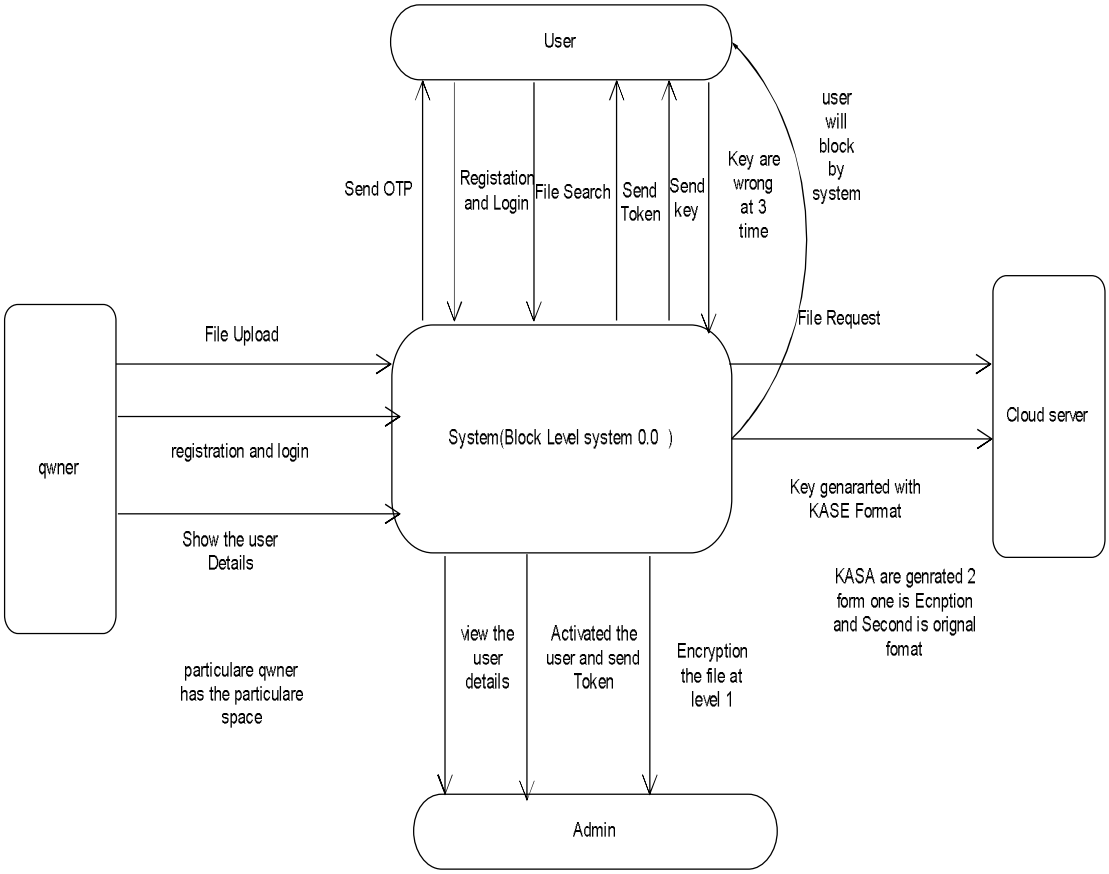
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

"Efficient public key encryption with revocable keyword search" Open key encryption with watchword look is a novel cryptographic rough engaging one to look for on the encoded data explicitly. In the known plans, once getting a trapdoor, the server can look for related data without any confinements. In any case, really, it is once in a while crucial to shield the server from glancing through the data all the time in light of the way that the server isn't totally trusted. In this paper, we propose open key encryption with revocable watchword chase to address the issue. We in like manner develop a strong improvement by dividing the whole presence of the system into specific events to achieve our destinations. The proposed plot achieves the properties of the caprice of cipher texts against a flexible picked watchwords ambush security under the co-decisional bilinear Diffie– Hellman assumption in our security illustrate. Differentiated and two somewhat plots, our own offers much better execution to the extent computational expense [15].

III. PROPOSED WORK



In Our System there are three role such as user, admin & cloud when, data are upload the file then encryption and admin encryption at content level then cloud take file and encryption at file level and generated the block of user and split file into multiple chunks and stored into block level. \\

In System there are four Roles in Application Data Provider, user, Admin, Cloud Server provider when Data Provider upload the Data in different Group while uploading the admin get the file and encryption at content level and Generated the key and that key and Data are send to Cloud server provider(CSP). When the Cloud Server Provider encryption at file level and Update the Key and Stored in different Group, When user search the Data from Cloud from different Group. When other user gets the Data from different group then reconstruction algorithm is applied on Data.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Algorithms:-

- **Block Generating (v, k+1, 1) :- generating a new block :-**

1. for i=0;i<=k;i++ do
2. for j=0;j<=k;j++ do
3. if j==0 then
4. $B_{i,j}$=0; else
5. $B_{i,j}$=ik+j;
6. end if
7. end for
8. .end for
9. for i=k+1 ;i<=k +k ;i++ do
10. . for j=0;j<k ;j++
11. .j==0 then
12. $B_{i,j}$=[(i-1)/k +1]
13. Else
14. B_i.k=jk+1 +Mod k+1(i-j+(j-1)[i-1]/k+1)
15. End if
16. End for
17. End for

- **Re-construction of B :- reconstruction of new Block :-**

1. E_0=B_0; Steps 1
2. For t=1;t<=k+1;t++ do
3. E_t=Btk+1 Steps 2
4. $B_{t,k}$=[Flag]=1;
5. E_{et},1=B[Et,t/ K] steps 2
6. $_{Btk}$+1[flag]=1
7. End for
8. For i=k+1 ;i<k+1; i++ do
9. If B_i[Flag]!=1 then
10. $E_{b,i}$[i+1/K]=Bi steps 3
11. End if
12. End For

- **Blowfish Algorithms**

1) Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

2) XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)

3) Encrypt the all-zero string with the Blowfish algorithm, using the data file described in steps (1) and (2).

4) Replace P1 and P2 with the output of step (3).

5) Encrypt the output of step (3) using the Blowfish algorithm with the modified data

6) Replace P3 and P4 with the output of step (5).

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

- **AES Algorithms :-**

1. Input:
2. 128 bit /192 bit/256 bit input(0,1)
3. Secretkey(128 bit)+plain text(128 bit).
4. Process:
5. 10/12/14-rounds for-128 bit /192 bit/256 bit input
6. Xor state block (i/p)
7. Final round:10,12,14
8. Each round consists:sub byte, shift byte, mix columns, add round key.
9. Output:
10. cipher text(128 bit)

Mathematical Model :-

1. S ={S1,dO,U,C,A,F,BC,Ca}
2. Here S1 is System and DO is data Owner, U is user and C is Cloud Server Provider and A is Admin f is File or data which stored in the Cloud.
3. BC is Block Chain which used to Store the data.
4. Ca is category which data are stored into different form in cloud.
5. Data Owner upload the file and Stored into different category
6. $W_k^i = w_k^i(c(i, P_k) + \sum_{(j \in R_k), j \neq i} c(P_{k,\ j}))$
7. MC generate MACfile and stores MACfile in local memory
8. MC uploads file on server
9. CSP stores file on cloud
10. MC sends request to CSP for performing insertion/deletion in the file
11. CSP sends requested file to MC
12. CSP forwards requested file to TCO
13. TCO sends MACtco to MC directly
14. MC compares MACfile and MACtco for verifying integrity (8): MC insert/delete a block in file and computes MAC for that block (9): MC uploads updated block on cloud (10): CSP stores updated file.

IV. RESULT

In this subsection, our System evaluate the performance of theproposed scheme by several experiments. system run these experiments on a window machine with an Intel Pentium 2.30GHzprocessor and 8GB memory. All these experiments use Java programming language with the many type of encryption algorithms such as AES and Blowfish Algorithms and also using Block Level Concepts. In our experiments, System first Install required Software. The Data are stored in the Block Level. In Block Level concepts the Data are stored into random block which generated by (SBIBD) Approach.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Metric	Existing system	Proposed System
Data Dynamic	No	Yes
Public Audit ability	Yes	Yes
Verifier Storage	No	Yes
Every time key Generation	No	Yes

Figure 1: Different between Different Entity with different Role

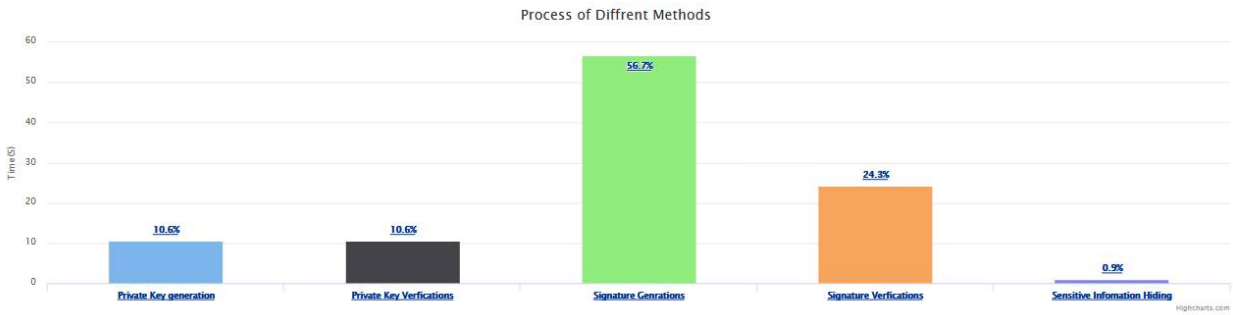
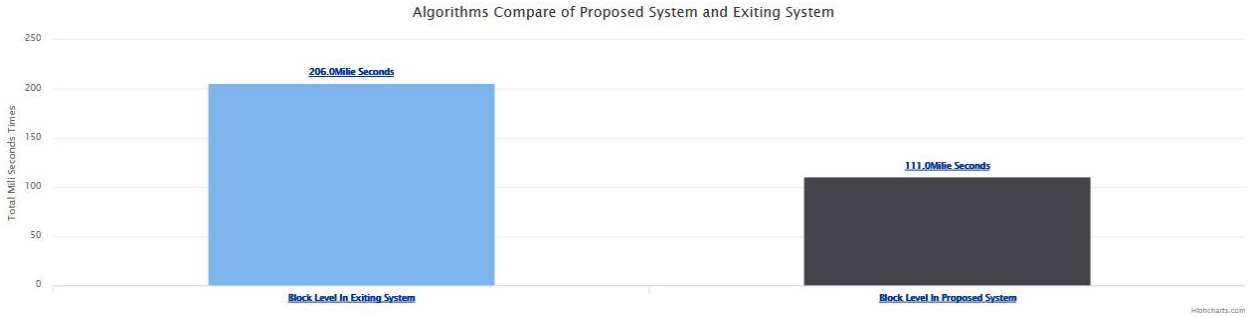


Figure 2: Graph between Algorithms

Here Exiting System Block Level and are not present in the only data are Stored into cloud but and Block level Concept stored the full data into single Cloud. In our proposed System data are drop then content level encryption is done and after data is stored into Block Level .



ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

V. CONCLUSION

As a development in the technology of the Internet and cryptography, group data sharing in cloud computing has opened up a new area of usefulness to computer networks. With the help of the conference key agreement protocol, the security and efficiency of group data sharing in cloud Computing can be greatly improved. Specifically, the outsourced data of the data owners encrypted by the common conference key are protected from the attacks of adversaries. Compared with conference key distribution, the conference key agreement has qualities of higher safety and reliability. However, the conference key agreement asks for a large amount of information interaction in the system and more computational cost..

REFERENCES

1) Y. Amir, Y. Kim, C. Nita-Rotaru, and G. Tsudik, "On the performance of group key agreement protocols," ACM Trans. Inf. Syst. Secur., vol. 7, no. 3, pp. 457–488, Aug. 2004.
2) D. Augot, R. Bhaskar, V. Issarny, and D. Sacchetti, "An efficient group key agreement protocol for ad hoc networks," in Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw., 2005, pp. 576–580.
3) A. Beimel and B. Chor, "Communication in key distribution schemes," in Proc. Adv. Cryptol., 1994, vol. 773, pp. 444–455.
4) R. Blom, "An optimal class of symmetric key generation systems," in Proc. Adv. Cryptol., 1984, vol. 209, pp. 335–338.
5) D. Boneh and M. K. Franklin, "An efficient public-key traitor tracing scheme," in Proc. Adv. Cryptol., 1999, vol. 1666, pp. 338–353.
6) D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in Proc. Adv. Cryptol ., 2005, vol. 3621, pp. 258–275.
7) D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," in Proc. 25th Int. Conf. Theory Appl. Cryptographic Tech., 2006, vol. 4004, pp. 573–592.
8) D. Boneh and M. Naor, "Traitor tracing with constant size Cipher text," in Proc. 15th ACM Conf. Comput. Comm. Security, 2008, pp. 501–510.
9) D. Boneh and A. Silverberg, "Applications of multilinear forms to cryptography," Contemporary Math., vol. 324, pp. 71–90, 2003.
10) C. Blundo, L. A. Mattos, and D. R. Stinson, "Generalized Beimel- Chor schemes for broadcast encryption and interactive key distribution," Theor. Comp. Sci., vol. 200, no. 1–2, pp. 313–334, 1998.
11) J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.
12) Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-K. R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," *IEEE Trans. Depend. Sec. Comput.*, to be published
13) J. Hur, D. Koo, Y. Shin, and K. Kang, "Secure data deduplication with dynamic ownership management in cloud storage," *IEEE Trans. Knowl.Data Eng.*, vol. 28, no. 11, pp. 3113–3125, Nov. 2016.
14) Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," *IEEE Trans. Depend. Sec. Comput.*, to be published.
15) H. Wang, D. He, J. Yu, and Z. Wang, "Incentive and unconditionally anonymous identity-based public provable data possession," *IEEE Trans. Serv. Comput.*, to be published.