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

Secure Data Distribution System in Cloud Computing Using Block Level

Attideep Raina, Vihan Parmar, Yamini Gaikwad, Prof. Pramod Jadhav

B. E Students, Department of Computer Engineering, Dr. D.Y.Patil School of Engineering, Pune, India

Professor, Department of Computer Engineering, Dr. D.Y.Patil School of Engineering, Pune, India

ABSTRACT:- Despite the fact that the electronic advancements have experienced quick improvements as of late, for example, cell phones are still nearly feeble as opposed to work areas as far as computational capacity, stockpiling and so forth, and are not ready to meet the expanding requests from versatile clients. By coordinating versatile registering and distributed computing, Mobile Cloud Computing (MCC) enormously broadens the limit of the versatile applications, yet it additionally acquires numerous difficulties in distributed computing, e.g., information security and information trustworthiness. Here, we using a few cryptographic natives, for example, another compose based intermediary re-encryption to outline a safe and efficient information conveyance framework in MCC, which gives information protection, information uprightness, information verification, and flexible information dissemination with control. We propose to actualize an extra idea of block chain in recovering keys in a chain arrangement and utilize adaptation to non-critical failure to maintain a strategic distance from interruption into the framework.

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

I.INTRODUCTION

With the undeniably large number of gadgets, for example, workstations, PDA's and tablets, clients require pervasive and enormous system stockpiling to deal with their regularly developing advanced lives. To meet these requests, much cloud-based capacity and record sharing administrations, for example, Drop box, Google Drive and Amazon S3 have picked up ubiquity due to the simple to-utilize interface and low stockpiling expense. In any case, these brought together distributed storage administrations are reprimanded for snatching the control of clients' information, which enables capacity suppliers to run investigation for promoting and publicizing One conceivable answer to decrease the danger of data spillage is to utilize multi distributed storage frameworks in which no single purpose of assault can release all the information. A vindictive substance, for example, the one uncovered in ongoing assaults on protection would be required to pressure all the diverse Cloud Server Provider on which a client may put his/her information, so as to get an entire image of his/her information. Put just, as the adage goes, don't put all the investments tied up on one place. However, the circumstance isn't so basic. CSPs, for example, Drop box, among numerous others, utilize Rsync-like conventions to synchronize the nearby document to remote record in their concentrated mists. Each neighborhood document is parceled into little pieces and these lumps are hashed with fingerprinting calculations, for example, SHA1, MD5 Thus, a record's substance can be remarkably recognized by this rundown of hashes. For each refresh of neighborhood record, just pieces with changed hashes will be transferred to the cloud. This synchronization dependent on hashes is not quite the same as like as conventions that depend on looking at two variants of a similar record line by line and can distinguish the correct updates and just transfer these updates in a fix style. Rather, the hash based

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

synchronization demonstrates necessities to transfer the entire lumps with changed hashes to the cloud. Subsequently, in the multi cloud condition, two pieces varying just somewhat can be conveyed to two distinct mists.

1.1 Background:-

This area completely investigates the thought and the design of the three primary cryptosystems, i.e. character based encryption, intermediary re-encryption, and part based access control that is utilized to characterize secure and dependable access control procedures in cloud and appropriated processing.

1.2 Motivation:-

1. One of the key factors that has led to motivating our ideas is primarily performing "Attributed Based Encryption", where encryption is prominently performed in two stages, one of which is content based encryption and the second one being fully encrypted based encryption system. This brings us to understand the very essence of encrypting essential information with maximum reliability in cloud computing.
2. Information is the new currency in today's generation, securing information is a formidable challenge and is also equivalently important. Hence, checking the integrity of the data is highly important. Efficiently exchanging and preserving data is a case of utmost importance in a rapidly growing information society.
3. With the widespread of information, a variety of data is freely available. Collection of various types of data, preservation of such a versatile data in a data world, transforming unreliable data into efficient data is a matter of grave importance. Similarly, securing this valuable information using various encryption schemes in cloud computing stands equal grounds. The demand for Data Security is highly increasing, as people are exponentially producing, using and exchanging data. With trusted sources, such as proving data security in cloud computing, we can create a global network of reliable sources for securing the data.
4. One of the most concerning issue is storing the data reliably, and providing the data to the customers as and when required, with maximum efficiency. In order to achieve such a desirable state of fluency, the mechanism to store data in the cloud holds a keen eye. With an integrated and a well-versed flexible mechanism, many of which can be administered using cloud, storing the data reliably and accessing the data at quantum speeds is a promising approach, which in turn leads to customer satisfiability and ingrains a trust-worthy system.
5. A highly administered cloud computing environment sheds light on accessing information securely. With this aspect, we can avoid data duplication and make sure that no person uses the information stored on cloud incorrectly. In order to maintain data integrity and sustain data security, we come across various access control rights, which are broadly divided amongst various roles participating in the system. These rights enable the system to understand the basic question; who, which, when and how the data is accessed. Having a clear

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

insight on such matters helps us maintain the integrity of the data and provide valuable services to the customers.

1.3 Aims and Objectives:

I. A primary aim is to use quick and reliable searching methods in order to increase data access speeds. With the help of which we can achieve a fast, fluent and a flexible storage and information access system, such as in cloud computing. The objective is to enhance efficient user communication with the system and provide satisfiable services to the users.

II. Preserving, accessing and exchanging information has now become an important factor in a rapidly growing business oriented and technology supported world. Information is exponentially produced every second by a billion technology users across the globe. In order to preserve valuable information, the society leans on reliable sources, one of which that is widely used is the cloud computing environment. The cloud computing environment aims to provide maximum security for the data the users want to preserve and compute efficient mechanisms in order to provide data reliability. One such mechanism that will be prominently used in our application is the use of Block level concepts, which will ensure data security, data integrity and data reliability.

III. Multiple data owners store their data in the cloud so as to ensure data availability at any time and at any place, to provide security to their valuable information, and to efficiently access their data. This data is highly versatile in its origin and managing such a variety of data is a matter of utmost importance. In order to achieve such broad end goals, there has to be an efficient mechanism to ensure that the data being preserved and accessed by the user doesn't alter from its origin, that the system ensures a safe, and a fault tolerant environment. Thus, in this application fault tolerances are used in order to provide maximum reliability and security for the data uploaded on the cloud by the Data Owner.

II.REVIEW OF LITERATURE

1. "Public key encryption with keyword search "We think about the issue of seeking on information that is encoded utilizing an open key framework. Consider client Bob who sends email to client Alice scrambled under Alice's open key. An email door needs to test whether the email contains the catchphrase "earnest" with the goal that it could course the email appropriately. As another representation, consider a mail server that stores diverse messages openly encoded for Alice by others. Using our instrument Alice can send the mail server a key that will enable the server to perceive all messages containing some specific catchphrase, anyway get nothing else. We describe open key encryption with watchword request and give a couple of improvements.

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

2. “Vabks: Verifiable attribute-based keyword search over outsourced encrypted data” Usually these days for information proprietors to outsource their information to the cloud. Since the cloud can't be completely trusted, the outsourced information ought to be encoded. This anyway brings a scope of issues, for example, How should an information proprietor give look abilities to the information clients? In what manner can the approved information clients seek over an information proprietor's outsourced scrambled information? By what means can the information clients be guaranteed that the cloud reliably executed the pursuit tasks for their sake? Propelled by these inquiries, we propose a novel cryptographic arrangement, called obvious characteristic based catchphrase look (VABKS). The arrangement permits an information client, whose accreditations fulfill an information proprietor's entrance control strategy, to (I) look over the information proprietor's outsourced encoded information, (ii) outsource the dreary pursuit tasks to the cloud, and (iii) confirm whether the cloud has dependably executed the inquiry activities. We formally characterize the security prerequisites of VABKS and depict a development that fulfills them. Execution assessment demonstrates that the proposed plans are viable and deployable.

3. Fuzzy identity-based encryptionWe 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 enlightening properties. A Fuzzy IBE conspire takes into consideration a private key for a character, ω, to decode a ciphertext encoded with a personality, ω 0 , if and just if the characters ω and ω 0 are near each other as estimated by the "set cover" remove metric.A Fuzzy IBE plan can be associated with enable encryption using biometric commitments as identities; the mix-up opposition property of a Fuzzy IBE plot is precisely what considers the use of biometric characters, which naturally will have some commotion each time they are analyzed. Also, we demonstrate that Fuzzy-IBE can be utilized for a sort of utilization that we term "trait based encryption". In this paper we display two developments of Fuzzy IBE plans. Our developments can be seen as an Identity-Based Encryption of a message under a few properties that form a (fluffy) character. Our IBE plans are both blunder tolerant and secure against conspiracy assaults. Also, our essential development does not utilize irregular prophets. We demonstrate the security of our plans under the Selective-ID security display
.

4. “Searchable encryption revisited: Consistency properties, relation to anonymous IBE and extensions”We recognize and fill a few holes as to consistency (the degree to which false positives are created) for open key encryption with watchword seek (PEKS). We characterize computational and factual relaxations of the current thought of impeccable consistency, demonstrate that the plan of is computationally steady, and give another plan that is measurably reliable. We likewise give a change of a mysterious IBE plan to a protected PEKS plot that, dissimilar to the past one, ensures consistency. At last we recommend three expansions of the essential

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

thoughts considered here, in particular mysterious HIBE, open key encryption with transitory catchphrase inquiry, and character based encryption with watchword look.

5. “Anonymous hierarchical identity-based encryption (without random oracles)”We show a character based cryptosystem that highlights completely unknown ciphertexts and various leveled key designation. We give a proof of security in the standard model, in light of the gentle Decision Linear multifaceted nature supposition in bilinear gatherings. The framework is effective and useful, with little ciphertexts of size direct in the profundity of the chain of importance. Applications incorporate pursuit on encoded information, completely private correspondence, and so forth. Our outcomes settle two open issues relating to unknown character based encryption, our plan being the first to offer provable secrecy in the standard model, notwithstanding being the first to acknowledge completely mysterious HIBE at all levels in the chain of importance.

6. “Efficient public key encryption with revocable keyword search” Open key encryption with watchword look is a novel cryptographic crude empowering one to seek on the encoded information specifically. In the known plans, once getting a trapdoor, the server can seek related information with no limitations. Be that as it may, actually, it is now and then fundamental to keep the server from looking through the information all the time in light of the fact that the server isn't completely trusted. In this paper, we propose the idea of open key encryption with revocable watchword hunt to address the issue. We likewise build up a solid development by partitioning the entire existence of the framework into particular occasions to accomplish our objectives. The proposed plot accomplishes the properties of the vagary of ciphertexts against a versatile picked watchwords assault security under the co-decisional bilinear Diffie– Hellman presumption in our security demonstrate. Contrasted and two to some degree plots, our own offers much better execution as far as computational cost.
7. “Practical techniques for searches on encrypted data”It is alluring to store information on information stockpiling servers, for example, mail servers and record servers in encoded shape to diminish security and protection dangers. Yet, this as a rule suggests that one needs to forfeit usefulness for security. For instance, if a customer wishes to recover just archives containing certain words, it was not already known how to let the information stockpiling server play out the inquiry and answer the question without loss of information classification.
8. “Secure indexes" A safe list is an information structure that permits a querier with a "trapdoor" for a word x to test in O(1) time just if the list contains x; The file uncovers no data about its substance without legitimate trapdoors, and trapdoors must be produced with a mystery key. Secure files are a characteristic expansion of the issue of building information structures with protection ensures, for example, those given by neglectful and history free information structures. In this paper, we formally characterize a protected record and figure 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

security display for files known as semantic security against versatile picked watchword assault (ind-cka). We likewise build up a proficient indcka secure list development called z-idx utilizing pseudo-irregular capacities and Bloom channels, and demonstrate to utilize z-idx to execute looks on encoded information. This inquiry plot is the most effective scrambled information look conspire right now known; It gives O(1) seek time per report, and handles compacted information, variable length words, and boolean and certain general articulation inquiries. The systems created in this paper can likewise be utilized to construct scrambled accessible review logs, private database inquiry plans, amassed hashing plans, and secure set enrollment tests..

9. “A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data” —In view of the growing reputation of circulated figuring, a regularly expanding number of data proprietors are impelled to outsource their data to cloud servers for unprecedented settlement and lessened cost in data organization. Be that as it may, delicate information ought to be scrambled before outsourcing for security prerequisites, which obsoletes information usage like watchword based record recovery. In this paper, we display a safe multi-catchphrase positioned look conspire over encoded cloud information, which at the same time underpins dynamic refresh tasks like erasure and inclusion of reports. Due to the usage of our remarkable tree-based document structure, the proposed plan can achieve sub-coordinate interest time and deal with the eradication and incorporation of files adaptably. Wide examinations are coordinated to display the adequacy of the proposed plot.
10. Privacy-preserving multi keyword ranked search over encrypted cloud data,” —With the coming of distributed computing, information proprietors are spurred to outsource their perplexing information administration frameworks from nearby locales to the business open cloud for extraordinary adaptability and monetary reserve funds. Be that as it may, for securing information protection, touchy information must be scrambled before outsourcing, which obsoletes conventional information usage in light of plaintext watchword seek. Subsequently, empowering a scrambled cloud information seek benefit is of principal significance. Thinking about the substantial number of information clients and records in the cloud, it is important to permit different watchwords in the pursuit demand and return archives in the request of their significance to these catchphrases. Related takes a shot at accessible encryption center around single watchword look or Boolean catchphrase seek, and once in a while sort the query items. In this paper, out of the blue, we characterize and take care of the testing issue of security protecting multi-watchword positioned look over scrambled cloud information (MRSE). We set up an arrangement of strict protection necessities for such a safe cloud information usage framework. Among different multi watchword semantics, we pick the proficient likeness proportion of "arrange coordinating", i.e., however many matches as would be prudent, to catch the pertinence of information archives to the pursuit inquiry. We additionally utilize "inward item similitude" to quantitatively assess such comparability measure. We at first propose a basic idea for the MRSE in perspective

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

of secure internal thing count, and after that give two out and out upgraded MRSE intends to achieve diverse stringent assurance requirements in two unmistakable threat models. Serious examination investigating insurance and profitability confirmations of proposed plans is given. Examinations on this present reality dataset furthermore demonstrate proposed plots for beyond any doubt exhibit low overhead on computation and correspondence

III. PROPOSED WORK

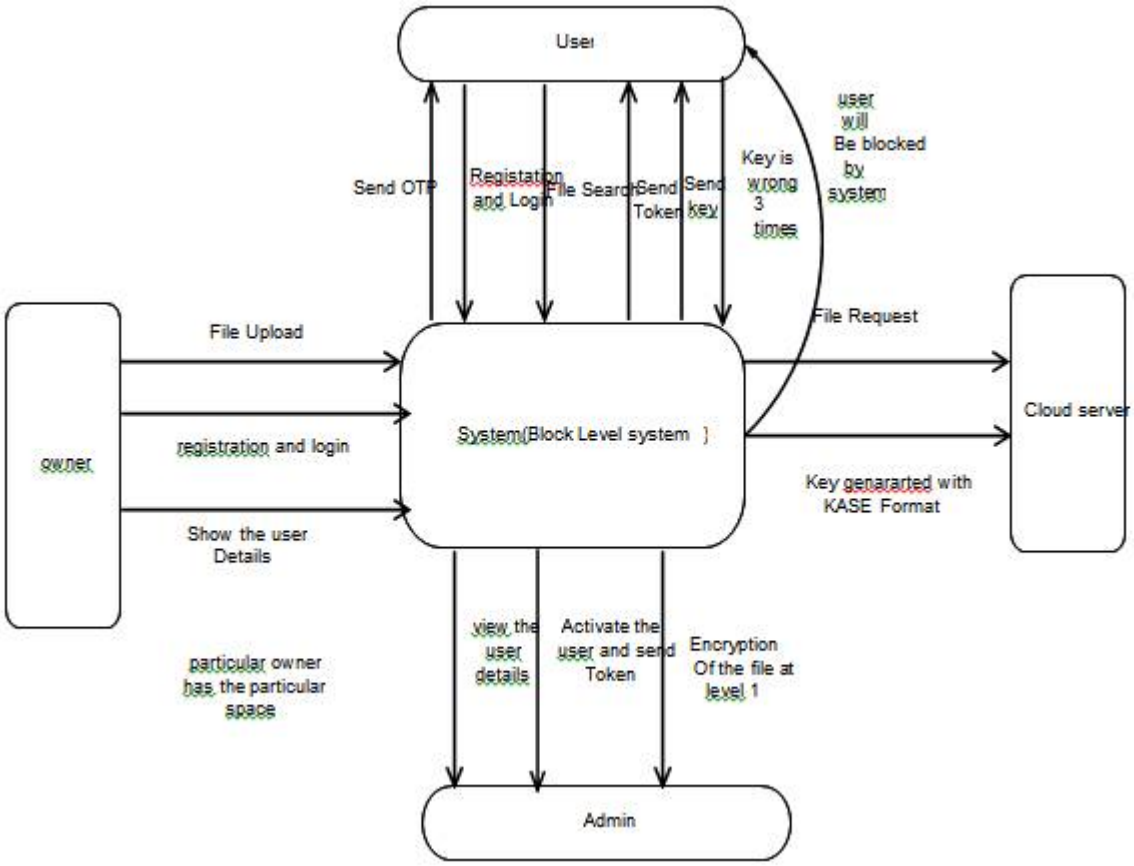

Fig 1: System Overview

In Block level Design there are four modules owner, user and Admin and Cloud Service Provider. User enters in application and registers and logs in, then admin activates the user and gives the token. After entering the token user logs in successfully. After login user searches the owner file and cloud Services Provider gives the Key in format of KASE. If user Enters the Wrong key (KASE) then level of fault Tolerances increases and if that 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

goes up to 3 then owner knows the user information and then the owner can block the that user. Then afterwards user is blocked from particular owner and the user is not able to get file of the particular owner.

There are four role in application such as the user, admin, owner and Cloud Server Provider. Whenever owner uploads data with Fault tolerances value then data encryption occurs at first level with AES Algorithm and after generating key cloud Server provider send the data into cloud with Block Level Algorithms.

3.1 System components: -

In the system that has been proposed above, there are three basic roles under which the project will be executed. All these three roles have autonomous control over the execution of the project. These roles are as follows:

1. Data Owner/User: 2. Administrator 3. Cloud Service Provider

Now, we shall elaborate these three roles independently,

1. Data Owner/User: The data owner/user will use a cloud service provider in order to efficiently store their valuable data and manage the data with maximum efficiency. The only thing that the data owner is concerned about is storing the data securely and retrieving the data reliably. Here, the data owner/user will upload a file, which may be of any type say; pdf, video, audio, or here we assume a text file. The data owner/user will simply upload the file on the cloud say 1.txt. The data owner has complete control of what data has to be uploaded and what data needs to be retrieved from the cloud. The moment the file is uploaded on the cloud, data encryption will be handy.
2. Administrator: An administrator is a person who manages the data uploaded by the data owner efficiently, so as to provide reliable data to the data owner/user. The job of the administrator is to manage the data uploaded by the data owner/user, provide encryption schemes to the data uploaded in order to maintain data integrity and reliability. The file uploaded by the data owner, i.e 1.txt is encrypted by the administrator. With the help of the encryption scheme used, the administrator will generate an alpha-numeric or a numeric or simply an alphabetic sequence say ‘x1y1z1’ and generate a key ‘K1’. This encryption will be performed at the content level and hence it is known as content level encryption. At the content level encryption, in order to decrypt the file content the data owner needs to first decrypt the key ‘K1’ to access the file content. The algorithm that is used to encrypt the data at the content level is “AES algorithm”.

   Further, the content level encryption i.e (x1y1z1+K1) is full encrypted and a new key is generated say ‘K2’. In order to decrypt this, ‘K2’ will be decrypted first and then ‘K1’ will be decrypted in order to access the file

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

content. This ensures maximum data security and reliability for the data owner/user. The algorithm that is used in order to provide full encryption i.e {(x1y1z1+K1)+K2} is “Blowfish algorithm”.

The fully encrypted file will be put into a block and will be split into multiple segments within the block. Note that data is split completely into various segments inside the block. This is done to avoid data replication in order to maintain data integrity, provide data security such that in case of unauthorized access, it is impossible to retrieve all parts of the data within different segments inside the block successfully.

In the block level, two main activities are performed; first one being the generation of a block for a new file to be split, second one being re-construction of the block if one file already exists and the second file needs to be split. There are two main techniques used in this entire system, thefirst one is “Fragmentation” which is used for splitting of the fully encrypted data into segments, the second one is “Merging” which is used at the content level using keys.

3. Cloud Service Provider: The file is uploaded to the cloud server, after the algorithms are applied on it for the process of encryption. After this if a user log in and wants to see a file or data of a particular data owner, it will search for the data owner‘s name in the application and then with the help of generated key, try to access it. At this point the system block will check whether the key is correct or not, if not and if the user puts a wrong key and crosses the fault tolerance value, the user will be blocked the system. If the right key is given, a file request will be generated to the cloud server and hence the user will access to the requested file.

3.2 Algorithms:-

The algorithms used in the proposed system are as follows:

1. Advanced Encryption Standard (AES) Algorithm 2. Blowfish Algorithm

Now, we will discuss the details of the above-mentioned algorithms.

1. Advanced Encryption Standard (AES) Algorithm: A popular and extensively used symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple Data Encryption Standard.A replacement for Data Encryption Standard was needed as its key size was very small. With an ever-increasing computational power, it was considered volatile against exhaustive key search attack. Triple DES was designed to overstep this drawback but it was found slow Advanced Encryption Standard is an iterative cipher. It works on the principle of ‘substitution–permutation network’.

Astonishingly, AES performs all its computations on bytes rather than bits. Thus, AES treats the 128 bits of a plaintext block as 16 bytes and then these 16 bytes are arranged in four columns and four rows for processing as a matrix.

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

a. Inputs:

1) 128_bit /192 bit/256 bit input(0,1)
2) secret key(128_bit)+plain text(128_bit).
3) 10/12/14-rounds for-128_bit /192 bit/256 bit input
4) XOR state block (I/P)
5) Final round:10,12,14
6) Each round consists: sub byte, shift byte, mix columns, add round key.

b. Output:

a. Cipher text(128 bit)

2. Blowfish Algorithm:

Blowfish Algorithm is a symmetric key block cipher. It was designed by Bruce Schneier, in the year 1993. It included a large number of cipher suites and encryption products. Blowfish algorithm provides a good encryption scheme in software and no effective cryptoanalysis of it has been discovered until now. However, AES now receives more attention, and Schneier recommends Twofish for modern applications.

Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging Data Encryption Standard and free of the problems and constraints associated with other algorithms. At the time when Blowfish was announced, many other designs were proprietary, encumbered by parents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in public domain, and can be freely used by anyone.

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

IV. RESULTS

In this subsection, our System evaluates the performance of the proposed scheme by several experiments. System runs these experiments on a window machine with an Intel Pentium 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the many type of encryption algorithms such as Min Hash and BFS Min Hash and also using Block Chain Concepts. The Data is stored in the Block Chain. In Block Chain concepts the Data are stored Sequentially into blocks which are generated by SP Chucking Algorithms.

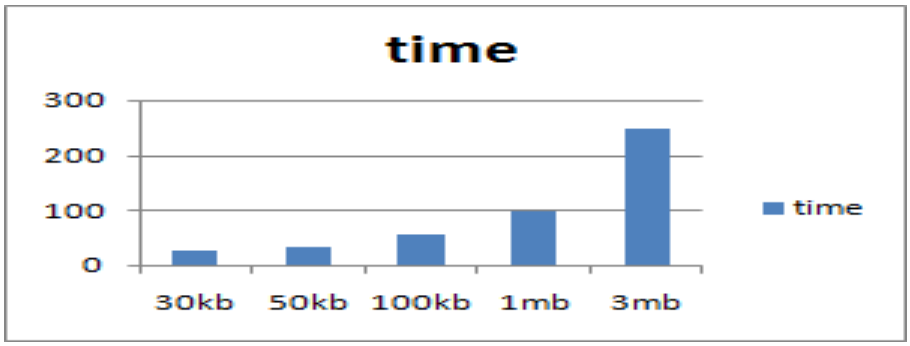

Fig 2: Shows file size on x axis and time (MS) to upload on Y-axis

Index Number	File size	Time in ms
1	30kb	30
2	50kb	35
3	100kb	60
4	1mb	100
5	3mb	250

Table 1: Show File Size and Time to Upload

Here, In Table 1 entity Analysis of person such as Admin, Cloud which performances different role. In Our System Data Owner Upload the Data in Dynamic Group which are show to Admin Side after show the Data “Click to Encryption” when User Request to Data access of Owner than System first Check Fault Tolerances Value and Then access To User.

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

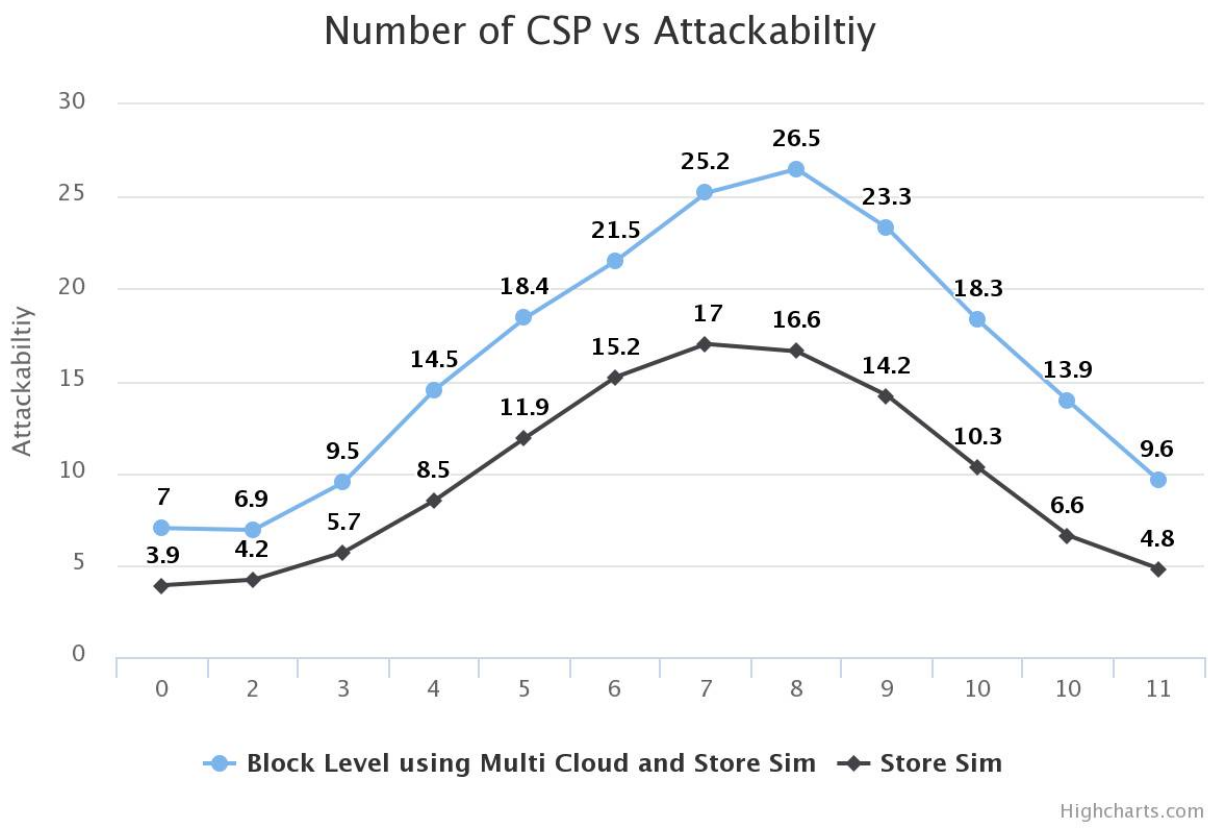

Fig3: Graph Between Number of CSP vsAttackabiltiy

IV. CONCLUSION

As advancements occur in the technology of 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 made immensely productive. 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. To counter the vulnerabilities in the conference key agreement, the SBIBD is used in the protocol design. Finally we have successfully designed and implemented a system with the help of AES and Blowfish Algorithm, SBIBD to enhance the security and privacy of user data.

REFERENCES

[1] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.
[2] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: Verifiable attribute-based keyword search over outsourced encrypted data," in INFOCOM, 2014 Proceedings IEEE. IEEE, 2014, pp. 522–530.
[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005. Springer, 2005, pp. 457–473.

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

[4] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions,"
in Advances in Cryptology–CRYPTO 2005. Springer, 2005, pp. 205–222.
[5] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption(without random oracles)," in Annual International CryptologyConference. Springer, 2006, pp. 290–307.
[6] Y. Yu, J. Ni, H. Yang, Y. Mu, and W. Susilo, "Efficient public keyencryption with revocable keyword search," Security and CommunicationNetworks, vol. 7, no. 2, pp. 466–472, 2014.
[7] Y. Yu, J. Ni, H. Yang, Y. Mu, and W. Susilo, "Efficient public key encryption with revocable keyword search," Security and Communication Networks, vol. 7, no. 2, pp. 466–472, 2014.
[8] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.
[9] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multikeywordfuzzy search over encrypted outsourced data with accuracyimprovement," IEEE Transactions on Information Forensics and Security,
vol. 11, no. 12, pp. 2706–2716, 2016.
[10] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamicmulti-keyword ranked search scheme over encrypted cloud data," IEEETransactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–
352, 2016.