International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5561
***Article Received**: 05 May 2022 **Revised**: 30 May 2022 **Accepted**: 20 June 2022 **Publication**: 31 July 2022*

Performance Development for Securing the Data Sharing Services in Cloud Storage using Hybrid Encryption

T. Thirumalaikumari, Research Scholar, School of Computing Science, VISTAS
Dr. C. Shanthi, (corresponding author) Associate professor, School of Computing Science, VISTAS

Abstract: Information sharing among more numbers of users especially the end clients. Preferable people will use famous and financially savvy cloud-based help for associations to share information with clients, and accomplices need of insider clients. This sort of administration further develops information accessibility and I/O execution by delivering and dispersing copies of shared information. Notwithstanding, such a strategy expands the capacity/network assets usage. At present, the Organizations have another choice to re-appropriate their monstrous information in the cloud without stressing over the size of information or the limit of memory. Be that as it may, moving classified and delicate information from believed person, area of the information proprietors by sharing with the public cloud will cause different security and protection chances. Moreover, the expanding measure of huge information reevaluated in the cloud builds the possibility to penetrate the protection and security of these data. Despite all the exploration that has been done around here, enormous information stockpiling security and security stays one of the main issues of associations that embrace computing and huge information technologies.

Keywords- Big data, Cyber security, Data Sharing, Decryption, Encryption.

1. Introduction

In cloud computing, authority acknowledges the client enlistment and makes a few boundaries. Cloud specialist co-op (CSP) is the supervisor of cloud servers and offers different types of assistance for the client. Information proprietor encodes and transfers the created cipher-text to CSP. Client downloads and decodes the intrigued cipher-text from CSP. The common records normally have a progressive design. That is, a gathering of records is separated into various progressive system subgroups situated at various access levels. In this process similar and various leveled construction could be scrambled by a coordinated admittance structure, the capacity cost of cipher-text and time cost of encryption could be saved. ID-based encryption is a notable methodology for encoded information.

Fig 1 Data Encryption – Private mode

This hybrid application schema consequently follows the benefits of ID-based methodology and works on the encryption of data. The ID-based encryption follows the private key, when a client endeavors to share information to companions, it is sensible that the client has the character (ID) of the companions, where the ID can be shared or accompany in record, an email address, a telephone number, as well as whatever address every interesting client. In ID-based encryption, the ID fills in as the public key of the beneficiary, along these lines complex key administration, authentication of the board, and endorsement check are not generally needed, and that implies that the sharing system is rearranged with proper security. Second, it is great to host a believed authority get-together and answerable for approval of big business perspective.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5561
***Article Received**: 05 May 2022 **Revised**: 30 May 2022 **Accepted**: 20 June 2022 **Publication**: 31 July 2022*

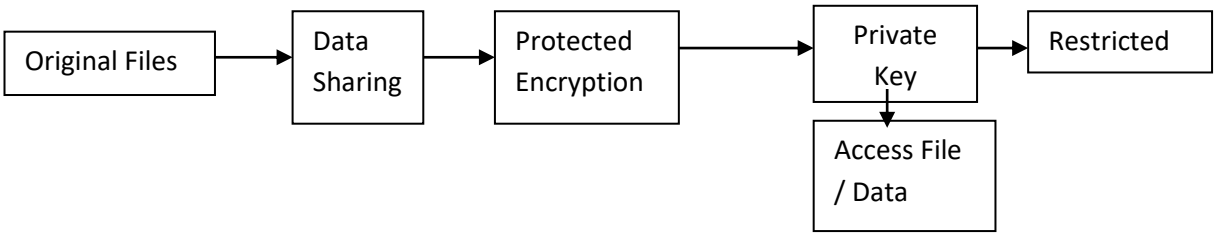

Fig 2 Hybrid Encryption Application Flow

For instance, just enlisted and approved clients can utilize the framework, another model just approved organization individuals can utilize organization reevaluated piling administration. ID-based cryptography requires confided outside person to create private keys for every user. A client can't do anything in event that the user doesn't have a private key in the framework. Third, ID-based encryption, public key encryption, different secure records and hidden entryways can be created regardless of whether the source watchwords are indistinguishable.

2. Literature Review

The played out a strategy for multi-authority intermediary re-encryption in view of code text-strategy quality based encryption (MPRE-CPABE) utilized for distributed storage plans. The technique needs information proprietor to convey each record into two squares that is one little square and one major square. To the huge one is scramble that used the little square. The private key is the name of large one. Then transformation takes place in the encoded enormous square to the distributed storage technique albeit the moved transferred huge square of record [1].

Identity based encryption (IBE) is the alluring cryptographic crude due to its pointless endorsement administrations. Nonetheless, in Identity-based encryption (IBE) the client dropping is one of the serious issues. To achieve disavowal, one potential methodology is utilized to refresh client's decoding keys. In any case, to forestall the necessity of secret channels, public keys time are expected to allow this update to happen. Character based encryption approach every now and again influences from two issues. 1) The client's save the straightly creating unscrambling keys. 2) Still, past code texts can access by the repudiated client to disavowal [2].

The introduced an arrangement of encoded information sharing for safe distributed storage framework, which relies upon the restrictive intermediary broadcast re-encryption innovation. The scrambled information sharing framework just not accomplish communicate information sharing framework through taking benefits of send encryption, additionally achieve dynamic sharing framework which empowers joining a client to and from the sharing sets, that a client is removing. Be that as it may, by using intermediary re-encryption innovation, the scrambled information sharing framework permits intermediary to share straightforwardly encoded information to point clients. Be that as it may, the information proprietor inclusion isn't needed while keeping information security. Consequently, the sharing exhibition is improved[3].

Graph encryption approach is examined for a fundamental inquiry type, which named as top-k Nearest Keyword (KNK) look. Many lists are intended to the necessary information is store for answer inquiries and affirmation that private information concerning the diagram. For e.g., catchphrases, vertex identifiers and edges are prohibited or encoded. Their diagram encryption framework, that confirmed effective and security through investigate the genuine datasets and hypothetical confirmations individually [4].In distributed storage, the essential issue is protection concerns and information security. In multi-client setting, in light of the homomorphism encryption, that played out the watchword search and provable public key encryption. The recommended strategy permits the server in DGHV homomorphism encryption to furnish a switched encryption list structure with no including question hidden entryway to productivity work on the pursuit [5].

Public key encryption by correspondence test (PKR-ET) empower to complete proportionality test among encoded the two message in light of discrete public keys. For the encryption public k, a property concealing predicate encryption is a model, which upholds both fine-grained admittance control and quality concealing methodology. At first lay out the trait concealing predicate encryption model and fairness test (AH-PE-ET) through adding the idea of PE and PKE-ET. Then, at that point, concrete AH-PE-ET framework is performed [6].

RSA Encryption and Decryption calculation is used to give cloud security. In RSA, while communicating the scrambled message, more data transmission is consumed. Thus to diminish the channel data transmission, the encoded message is sent into a limitless number of encoded bits utilizing Fountain Code. The reenactment results show an

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5561
***Article Received**: 05 May 2022 **Revised**: 30 May 2022 **Accepted**: 20 June 2022 **Publication**: 31 July 2022*

exceptional exhibition while utilizing Fountain Code RSA calculation than the conventional RSA calculation utilized for cloud security. Bundle Loss Ratio, Packet Delivery Proportion, Throughput, Residual Energy and End-to-End Delay shows an exceptional exhibition while utilizing Fountain code than in utilizing the conventional technique. The energy consumed in Fountain Code RSA calculation is less when contrasted with conventional RSA calculation. In this manner, the Fountain code RSA can be a best choice to cloud security strategies utilized as of now [7].

The point towards perceiving the dangers implied in information partaking in the cloud climate empowers the enhancements in information security, data integrity, and secrecy and client protection.This framework wants to additionally propose a framework improvement for the equivalent. The proposed framework is relied upon to further develop security levels further in distributed computing and capacity [8].

A solid information sharing plan, for dynamic gatherings in an un-believed cloud conspire permits a client to impart information to others inside the gathering without uncovering information and character security to the cloud. Moreover, it upholds proficient client renouncement and new client joining. All the more explicitly, proficient client renouncement can be accomplished through a public repudiation list without refreshing the private keys of residual clients and new clients can straightforwardly decode documents from the cloud previously their cooperation[9].

An elective answer for forestall the data spillage on the off chance that of conspiracy is to appropriate the portions of private key of Bob among different mists and Bob (Threshold Cryptosystem). One potential augmentation of our work is to foster a mixture approach by combining the information and key circulation arrangements. The proposed structure in cloud data changes for further assessment [10]. Manage group for dynamic key oriented towards the invitation of communication in asynchronous model management which provides key in dynamic way presentation of communication to the end user [11].

To safeguard information protection, an essential arrangement is to encode information documents, and afterward transfer the scrambled information into the cloud. A few security plans for information sharing on un-believed servers have been proposed. In these methodologies, information proprietor's store the scrambled information documents in un-confided away and disperse the comparing unscrambling keys just too approved clients. In this way, unapproved clients as well as capacity servers have no information on the substance of the information documents since they have no information on the decoding keys [12].

This work centers on "distributed computingcapacity administrations". Appropriately, cloud information isn't just put away in the server, yet regularly divided between an enormous numbers of clients in a gathering. In this paper, the creators propose Knox, a protection saving examining instrument for information put away inthe cloud and divided between an enormous numbers of clients in a bunch. Specifically, the plan uses the gathering marks to build homomorphic authenticators, so a Third Party Auditor (TPA) can confirm the honesty of the shared information. The personality of the underwriter on each square in shared information is kept hidden from the TPA [13].In distributed computing, the Cloud Service Providers (CSPs) can convey different administrations to cloud clients with the help of strong server farms. By transferring the nearby information the board frameworks into cloud servers, clients can appreciate top caliber of administrations and can save hugespeculations on their neighborhood foundations. One of the most key administrations presented by cloud specialist organizations as specialized one [14]. "Cryptographic Storage Service (ACSS)" which considersthe issue of building a solid distributed storage administration on cloud foundation where the specialist co-op isn't completely trusted by the client. It is comprised of three fundamental parts and acknowledges encryption stockpiling and trustworthiness approval by a gathering of conventions. Nonetheless, ACSS is hard to work since it bargains at a significant level and requires alteration of enormous measure of source code of cloud capacity stage [15].

3. Methodology

A new scheme that upgrades the security and protection of large information partook in cloud climate utilizing an entrance control scheme. Firstly, the plan ensures security and approved admittance of shared delicate information. Also, the plan acknowledges effective respectability confirmation before clients share the information to keep away from inaccurate calculation. At last, the plan accomplishes lightweight tasks of any terminals on the two information proprietor and information requester sides. The energy is decreased involving Energy-Efficient Virtual Machines Scheduling in Multi-Tenant Encrypted Data projection with private key. The proposed plot for these cycles is carried out utilizing and execution tried for the accompanying measurements: Information Loss, Compression Ratio, Encryption Time and Decryption Time.

A. Data Upload

In this hybrid scheme application, the information of user is safely store their restricted information on the semi-believed cloud specialist organizations, and specifically shared their

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5561
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

restricted information with a wide scope of information recipient. Data transfer to user – both records and information.

B. Encryption

It is generally late way to deal with reexamines the idea of Public-key cryptography as mystery key cryptography. In our mystery key cryptography, a message is scrambled for a particular collector utilizing the FH-ABE and the encryption is relies on information user trait. Information can be scrambled concerning subsets of traits. After the encryption cycle the information will part into 6 sections and put away in an alternate division in the cloud (server farms). The key is produced in light of the proprietor's property and the server farms esteems, the individual who holds the first key with the "matching qualities" can ready to unscramble the record and consolidation the dispersed documents.

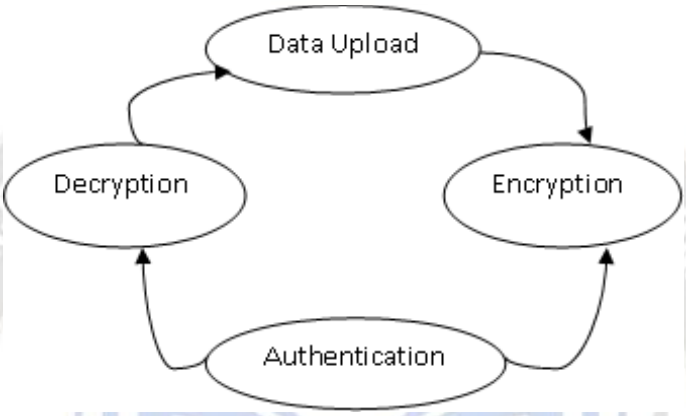

Fig 3 Methods Involved

C. Authentication

Cloud agents have been as of late presented as an extra computational layer to work with cloud determination and administration the executive errands for cloud customers. In any case, existing business plans on cloud administration choice regularly accept that merchants are totally trusted, and don't give any assurance over the rightness of the assistance suggestions. In this module the power will check the information beneficiary's full subtleties climate individual in ideal individual or cloud intermediary. The information recipients need to send demand for the record which needs to download. Information supplier really look at the subtleties, to impart the first record to the information beneficiary he will acknowledge the solicitation. On the off chance that the information proprietor not acknowledges the beneficiaries demand implies, even the information beneficiary won't get the download choice.

D. Decryption

The information recipient will download the vital when the information proprietor acknowledges the solicitation; the information beneficiary will involve the key for decoding and converging of the record. We will approve the information collector's data and record ascribes by utilizing of the first key with matching of the information proprietor's document characteristic and data. On the off chance that the first key approval is effectively finished, it naturally creates another two keys in the joined arrangement, it is chiefly for unscrambling and consolidation the document

4. Results and Discussion

In this data storage on cloud, asynchronous path of the uploaded file is made synchronous by processing the hybrid data scheme application using encryption propagation. This calculation picks a bilinear gathering G0 of prime request p with generator g. Each trait is then planned to a component of gathering G0. Give hi,b signify the comparing component access bunch G0 of property attribute b. hi,0 = ga1 and hi,1 = gb1, where computer based intelligence and bi are haphazardly produced from Zp. Let γi = computer based intelligence +bi. Simulated intelligence and bi ought to be picked in the manner that simulated intelligence, bi, and γi are for the most part non-unimportant. This calculation additionally picks other two arbitrary numbers α,β - Zp. The framework ace key (MK) is yield as follows

$$MK = (\alpha,\beta, \{ai, bi\} \forall i \in Zn)$$

A. Execution Steps

1. Each and every user had individual form of access login which are as follows

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5561
***Article Received**: 05 May 2022 **Revised**: 30 May 2022 **Accepted**: 20 June 2022 **Publication**: 31 July 2022*

Administrator

Random Number Generation, Chooses and upload random or sequential numbers s_0, s_1, …., s_{n-1}, controlling random files and data from the user. Administrator would get both upload access and file control access in the login.

----------$\sum_{j=0}^{n-1} X \gamma_i s_i$. ----------

User / Client

Request for the access of file - get proper permission from the respective person of the file and finally download file after request and permission. C_i is a Client of the form $C_i = (g^{si}, C_{i,0}, C_{i,1})$ and s_i is a random number generated in step 1. Both $C_{i,0}$ and $C_{i,1}$ are elements of group- computational request.

Table 1 Client Computation

	g^{s_i}	$C_{i,0}$	$C_{i,1}$
C_3	g^{s_3}	$g^{k_0} h_{3,0}^{s_3+t_3}$	$g^{k_1} h_{3,1}^{s_3}$
C_2	g^{s_2}	$g^{k_0} h_{2,0}^{s_2}$	$g^{k_1} h_{2,1}^{s_2+t_2}$
C_1	g^{s_1}	$g^{k_0} h_{1,0}^{s_1}$	$g^{k_1} h_{1,1}^{s_1}$
C_0	g^{s_0}	$g^{k_0} h_{0,0}^{s_0}$	$g^{k_1} h_{0,1}^{s_0+t_0}$

Super Administrator

Super Administrator controls the entire upload data of the application without any interruption from new upload. Pairing Aggregation: Total the Fi's and figure another worth F as follows:

F=∏_(i=0)^(n-1) F_i=∏_(i=0)^(n-1) e

2. Admin can transfer record and control document access for client

3.User can demand record and get permission for document from record proprietor and get access key to download document.

4. Super administrator can handle whole application

1. Control client/administrator login

2. Protected document access

3. All record are scrambled

4. Storage away in S3 bucket

Step I: Initialization ()

1: Method Initialization ( )

2: Initialize figure list classes with its document size

3: Generate public key by utilizing rundown of code file class and traits, produce irregular list

4: Generate other key by utilizing rundown of code file class and traits, produce irregular list

5: for each i=0 where i<bytes1.length

6: String j= figure record class name + arbitrary (I);

7: String str= Integer.toBinaryString (j)

8: increase I;

9: end for

10: end Procedure

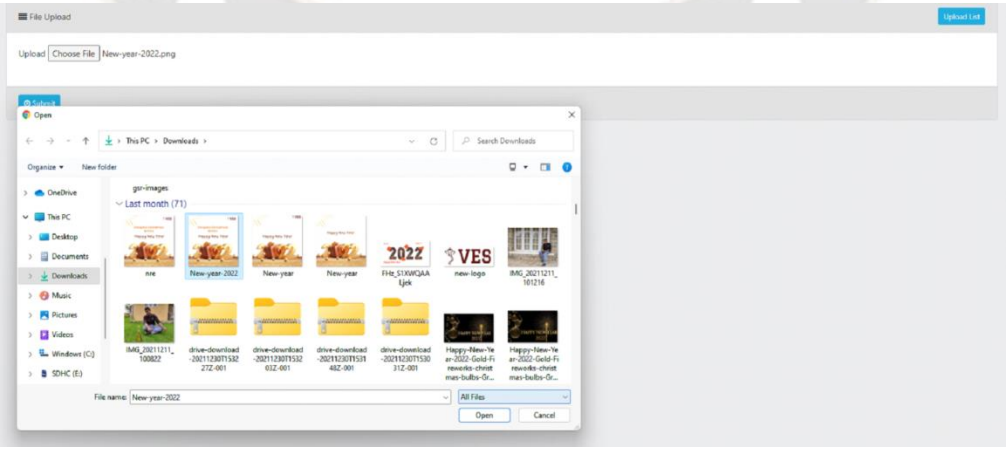

Fig 4 Original File

In Fig 4 the original file has been shown to differentiate the encrypted file with the unaligned improper formation of the direct uploaded file of the user. These data are immortal and non-uniform.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5561
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

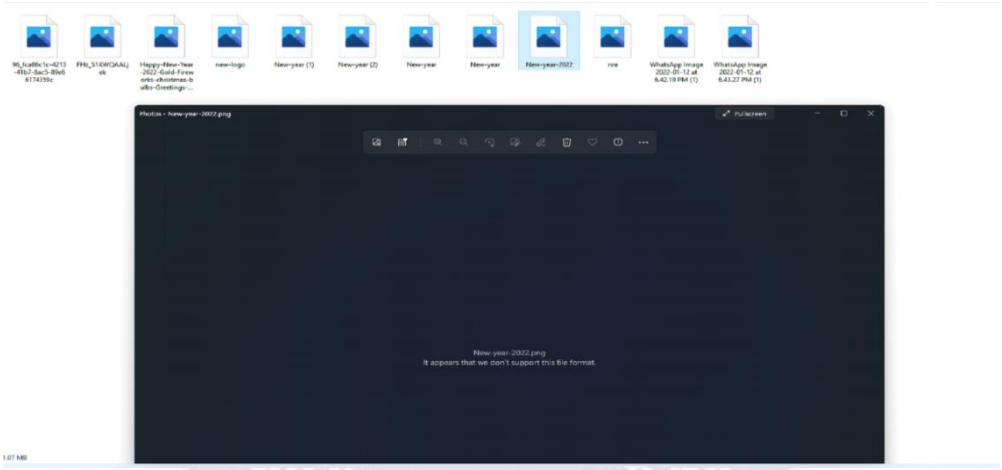

Fig 5 Encrypted file – Security

In Figure 5, the uploaded file in the hybrid schema would not be able to open from the public ID since it is encrypted from the application of cloud. Access is restricted to other rather than administrator, super administrator and user/ client.

Step II: Encryption of record

1: Procedure Encryption (b)
2: key instatement
3: Takes entire record as msg
4: FOS=new FileoutputStream (out)
5: byte [] b=new byte [8];
6: int I-cis.read (b);
7: while I! = - 1 do 8: fos.write (b, 0, I);
9: i=cis.read (b);
10: end while
11: end Procedure

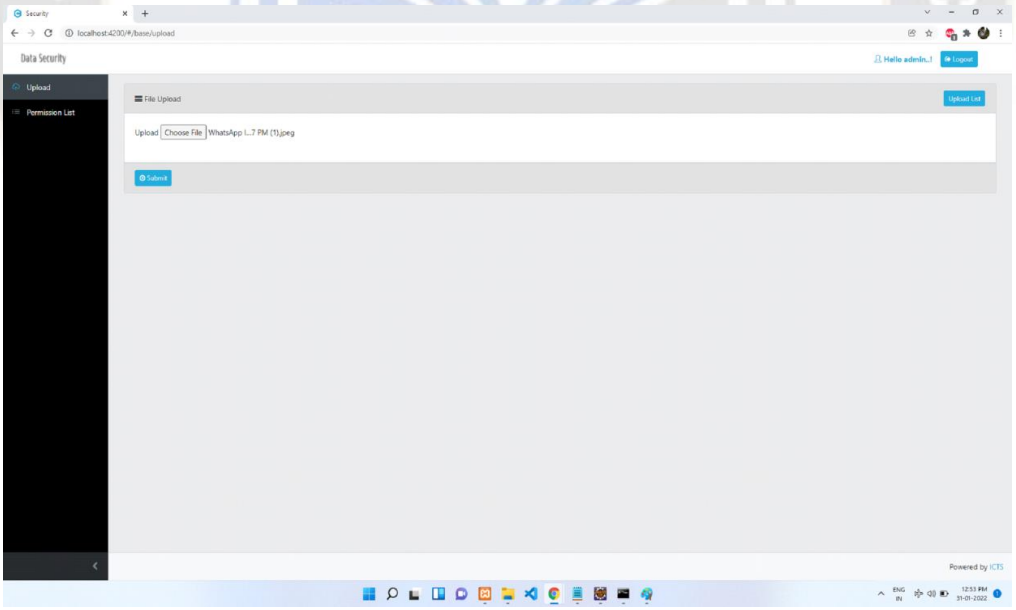

Fig 6 Admin Page

In Fig 6, Admin page has been shown this page will be visible only to the person who had access to it other person would only see the black restricted page.

Data Splitting Algorithm (Cryptographic Data Splitting)

Cryptographic information parting is another way to deal with getting data. This interaction encodes information and afterward utilizes arbitrary or deterministic appropriation to numerous offers. This dissemination can likewise incorporate issue open minded pieces, key parting,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5561
***Article Received**: 05 May 2022 **Revised**: 30 May 2022 **Accepted**: 20 June 2022 **Publication**: 31 July 2022*

verification, honesty, share reassembly, key reclamation or unscrambling.

1. Sign in and secret phrase access frequently doesn't give sufficient security.
2. Public-key cryptographic framework dependence on the client for security.
3. Private keys put away on hard drive that is available to other people or through the Internet.
4. Private keys being put away on a PC framework designed with a documenting or reinforcement framework that could bring about duplicates of the private key going through various PC stockpiling gadgets or different frameworks
5. Misfortune or harm to the smartcard or compact processing gadget in biometric cryptographic frameworks
6. Probability of a pernicious individual taking a versatile client's smartcard or compact registering gadget utilizing it to actually take the portable client's computerized qualifications.
7. The processing gadget association with the Internet might give admittance to the document where the biometric data is put away making it helpless to think twice about client distractedness to security or vindictive gatecrashers.
8. Presence of a solitary actual area towards which to concentrate an assault.

Step III Key page

1: Procedure Summation Keygen ( )
2: Masking public key and byte design
3: Masking insurance key and byte design
4: for each i=0 upto i<byptes12.lenght
5: int j=bytes12 [i];
6: String s3=Integer.toBinaryString (j);
7: String temp= temp + Integer.parseInt (s3);
8: S3=toBinaryString (temp);
9: end for
10: end Procedure

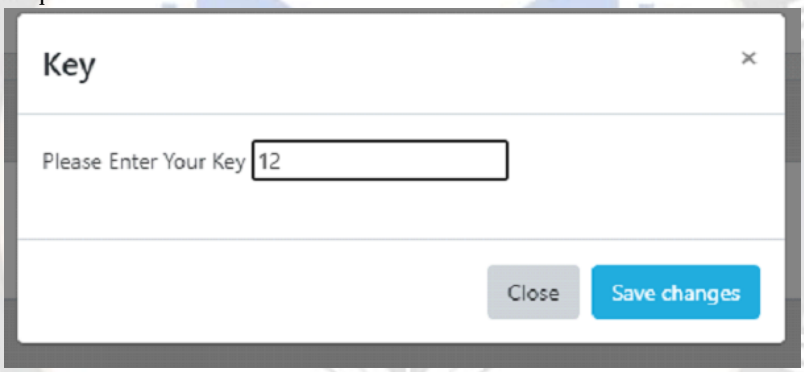

Fig 7 Private Key

In Figure7, Key page is for private purpose only the accessed person would get the key to enter. Each individual would have a separate secret key to enter. Keys are most of all would be numbers either two digital or multi digit.

Step IV: Decryption of record

1: Procedure Decryption (b)
2: Encrypt. nit (cipher.DecryptMode, Secret key);
3:Encrypt. nit (cipher.DecryptMode, Protected key);
4: cis=new fileOutputStream (fis, encode);
5: fos=new fileOutputStream (dec);
6: byte [ ] b=new byte [8];
7: inti=cis.read (b);
8: while I! =-1 do
9: fos.write (b, 0, I);
10: i=cis.read (b);
11: end while
11: end Procedure

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5561
***Article Received**: 05 May 2022 **Revised**: 30 May 2022 **Accepted**: 20 June 2022 **Publication**: 31 July 2022*

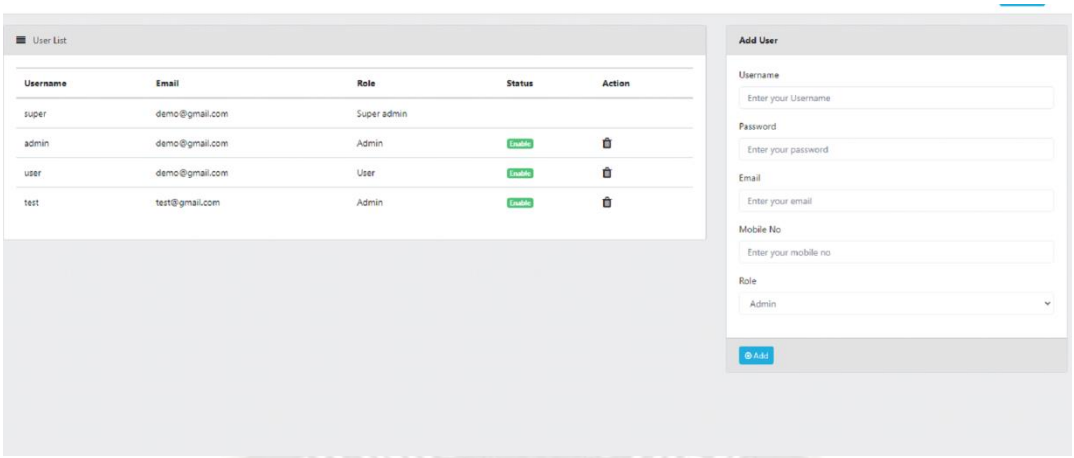

Fig 8 Overall views of the uploaded files

Above view of the uploaded file would be seen only by the super administrator, since the entire access of the application is given only to them. This overall view covers the entire uploaded file and data of the user which time initiated the upload, when the data is modified, viewed each and every detail would be seen by the super administrator and keep every detail secretly to maintain security for the user official and person data storage in cloud mapping with hybrid terminology.

Conclusion

In the recent epoch gigantic development of touchy data on cloud data sharing without privacy, cloud security is getting more significant than even previously. The cloud information and administrations live in greatly versatile server farms and can be gotten to all over. The development of the cloud clients has no personal information hiding on the development basis in noxious movement in the cloud. An increasing number of weaknesses are found, and virtually consistently, new security warnings are distributed. A huge number of clients are searching the cloud for different purposes, in this way they need exceptionally protected and relentless administrations. The fate of the cloud, particularly in growing the scope of uses, includes a lot further level of protection, and validation. This scheme of encrypted cloud application has developed onan advanced informative assurance model where information is scrambled utilizing key-approach on attribute-based encryption before it is sent off in the cloud, subsequently guaranteeing information privacy and security.

References

[1]. X. Xu, J. Zhou, X. Wang, and Y. Zhang, "Multi-authority proxy re-encryption based on CPABE for cloud storage systems," J. Syst. Eng. Electron., vol. 27, no. 1, pp. 211–223, 2016.

[2]. Y. Sun, W. Susilo, S. Member, F. Zhang, and A. Fu, "CCA-secure Revocable Identity-based Encryption with Cipher-text Evolution in the Cloud," IEEE Access, vol. PP, no. c, p. 1, 2018.

[3]. L. Jiang, D. Guo, and S. Member, "Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage," IEEE Access, vol. 14, no. 8, pp. 1–9, 2017

[4]. C. Liu, S. Member, L. Zhu, J. Chen, and S. Member, "Graph Encryption for Top-K Nearest Keyword Search Queries on Cloud," IEEE Trans. Sustain. Comp., vol. 3782, no. c, pp. 1–11, 2017

[5]. D. N. Wu, Q. Q. Gan, and X. M. Wang, "Verifiable Public Key Encryption with Keyword Search based on Homo-morphic Encryption in Multi-user Setting," IEEE Access, vol. 3536, no. c, pp. 1–9, 2018.

[6]. J. Sun, Y. Bao, X. Nie, and H. Xiong, "Attribute-hiding Predicate Encryption with Equality Test in Cloud Computing," IEEE Access, vol.6, pp.31621-31629, ISSN: 2169-3536, 2018.

[7]. A. Manimaran , K. Somasundaram, "An Efficient Secure and Flexible Data Sharing in Cloud Computing using Asymmetric Algorithm", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.9, Issue.4, pp. 411-415, ISSN: 2278-3075, 2020.

[8]. Kadam Prasad, Jadhav Poonam, Khupase Gauri, Prof. N. C. Thoutam, "Data Sharing Security and Privacy Preservation in Cloud Computing", International Conference on Green Computing and Internet of Things (ICGCIoT), IEEE,pp.1070-1075, 978-1-4673-7910-6, 2015.

[9]. Pawan Kumar Tiwari, P. S. . (2022). Numerical Simulation of Optimized Placement of Distibuted Generators in Standard Radial Distribution System Using Improved Computations. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 10–17. https://doi.org/10.17762/ijrmee.v9i5.369

[10]. Mahesh A., S. Balaji, "Secure Data Sharing for Dynamic Groups in the Cloud", International Journal of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v10i7.5561
Article Received: 05 May 2022 Revised: 30 May 2022 Accepted: 20 June 2022 Publication: 31 July 2022

Engineering Research & Technology (IJERT), ISSN: 2278-0181, pp.96-98, 2014.

[11]. Bharath K. Samanthula, Gerry Howser, Yousef Elmehdwi, and Sanjay Madria, "An Efficient and Secure Data Sharing Framework using Homomorphic Encryption in the Cloud, IEEE, 10.1145/2347673.2347681, 2012.

[12]. Lam, S.S-zebeni, and L.Buttyan, "Invitation-oriented: Key management for Dynamic groups in an asynchronous communication model", Submitted to 4th International Workshop on Security in Cloud Computing, 2012.

[13]. N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service" , Proceedings of IEEE (INFOCOM 2012), pp. 693–701, 2012.

[14]. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with large Groups in the Cloud," in the Proceedings of ACNS 2012, June 2012,

[15]. Taka-bi , H.; Joshi, J.B.D.; Ahn, G.; , "Security and Privacy Challenges in Cloud Computing," Security& Privacy, IEEE, vol.8, no.6, pp.24-31, doi:10.1109/MSP.2010.186, 2010.

[16]. Kamara, Seny and Lauter, Kristin, Cryptographic cloud storage, FC'10 Proceedings of the 14th international conference on Financialcryptograpy and data security, pp.136-149, 2010.