Research Article

Research on Encryption and Key Aggregate Searchable Decryption Methods for Data Storage in Cloud Securely

Akhila. H. Kumar[1],Manjunath C R[2]

PG student[1] Department of Computer Science and Engineering Jain (Deemed –To –Be University), Bangalore, Karnataka

Associate professor[2] Department of Computer Science and Engineering Jain (Deemed –To –Be University), Bangalore, Karnataka

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract-- In today's global, several corporations use data structures for their management of strategic and enterprise-important information. This kind of crucial problem wishes to be covered. no precedence can be given to the company. cloud computing ensures to extensively alternate the method we generally tend to use computers, access and preserve our private and industrial employer info. With this new computing and communications, paradigms arise brought statistics protection challenges. present statistics protection mechanisms have barriers in stopping records felony assaults, particularly those perpetrated with the aid of the usage of partner diploma agency executives to the cloud supplier to watch facts get right of entry to inside the cloud and find out peculiar facts get proper of entry to styles. Those kinds of challenges need to be addressed by the manner of growing a gadget with robust safety and privateness for cloud facts storage and facts sharing thru an encryption process. The variation to cloud-sharing files for the person for an encryption key technique to be used for lots of documents. Now, not entirely the encryption keys but additionally, the search keys need for use, and customers ought to maintain their keys impervious and disbursed. The present-day gadget the owner of the fact can solely percentage one key with the consumer, whether or no longer it's miles any kind of file, massive or small variety of documents, and the characteristic of the person is to cross a trap inside the cloud of ordinary overall performance finding out and safety evaluation of shared files, that's an impenetrable and great proposed gives schemes. And clients are additionally very concerned about information sharing garages, unexplained information leaks inside the cloud, and malicious attackers. In this paper, a trial has been made to layout an encryption mechanism for impenetrable records sharing.

Index Terms-- cloud data security, cloud data protection share, data leakage, encryption keys, single trapdoor, KASE scheme.

I. INTRODUCTION

Agencies gather large portions of records, from private commercial enterprise, economic, and customer statistics to non-vital data. The capacity to selectively share encrypted facts with quite a number customers via public cloud storage can drastically reduce safety issues with extraordinary information leaks in the cloud. The humans face several protection demanding situations, as nicely because the achievable for protection breaches, loss or thievery of touchy statistics and app crashes, and virus transmission. nowadays, numerous clients regularly proportion their records including videos, audio, files, files, folders, etc. the use of cloud storage. The primary motive for the software program is to permit surroundings-pleasant and invulnerable data sharing the usage of the concept of the usage of cloud computing as an vital hassle-solving task. As a while, clients try to upload documents, folders, pics, motion pictures, and many others. The uploading documents will produce one key and whilst downloading will generate some different protection keys referred to as cryptography cloud garage.

Right here, the cloud company company is the drop discipline however proper here the prevailing-day use could be very hard for clients to use so right here through using taking the driving force HQ as a cloud service agency will be useful for educational and corporation functions. However, statistics encryption makes it hard for clients to search and select for statistics most effective. Key terms furnished and a frequent reply is to rent a searchable encoding (se) theme the vicinity the statistics for information owner is needed to cipher conceivable key phrases and transfer them to the cloud with encrypted data, that, in retrieving statistics like key-word, the man or woman can deliver the corresponding key-phrase to the cloud.

Fig.1 Data Sharing

Considered one of the biggest issues managing the business agency these days is in gaining access to manipulate and searchable encryption. Right here, the focal factor in this hassle based on the information robbery attack inside the cloud with the aid of identifying the protection problem. Considering maximum customers are rectangular measure cognizant of this risk inside the cloud, all this is although is to have faith the provider supplier as soon as defensive their understanding. Knowledge house proprietors business company have a whole lot of sensitive records square degree the supply of our facts understanding cloud.

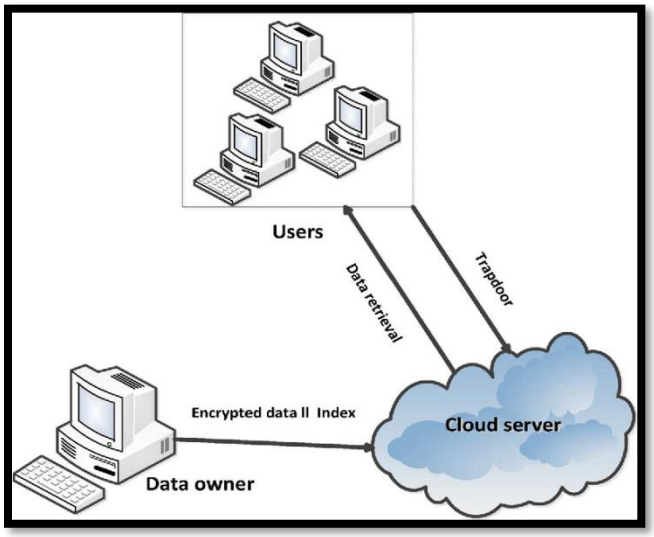


Fig.2 Cloud data secured sharing

To provide safe and privacy, such sensitive statistics are commonly encrypted in advance than our sourcing. Searching via encrypted statistics can moreover grow to be a undertaking. Right here, there will have a examine many records customers and record archives inside the cloud and there have to be a search issuer that lets in more than one keyword queries and generates rank consequences for recovered documents. Structures region unit designed to phrase and save you unauthorized use and transmission of course. All through this paper, the research worker offers with every one of the phrases facts loss and facts outflows in examining, on the other hand, the KASE technique enables minimizing the information larceny attacks while storing and sharing in the cloud.

A. PROBLEM DEFINITION

The information attacks while storing and sharing ought to end up in modern trouble in many businesses. That is an correct idea and the number one hassle from the organizational standpoint. That is specifically actual when a hassle arises in the safety mannequin that protects touchy records and agency /personal files. In the business enterprise, the most vital reality loss is on the whole because of inner assaults. Notwithstanding protection implemented sciences like firewalls, IDS, etc. (already done in the business enterprise) are very effective. Because these techniques don't assist interior attacks, so it is able to result in fact leak troubles. If you take a look at the top of a disadvantage to

avoid data leakage problem is it what to deal with in the route of this issue? It is presently clear that the records should be covered in competition to records loss to supply an aggressive facet. The problem, a manner to prevent the statistics leak, searchable approach, and getting access to disadvantage while storing and sharing in the cloud.

II. EXISTING SYSTEM

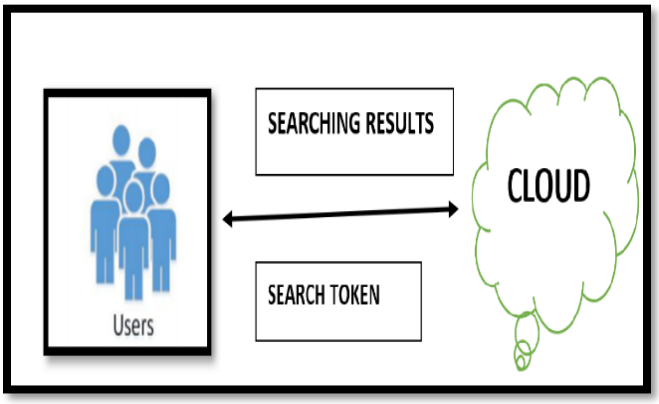


Fig3. Search over ciphertexts encrypted

By the usage of the idea of identification-based totally encryption with equality check assisting flexible authorization (IBEET-FA) algorithm, [1]building IBEET-FA schemes without the use of bilinear pairing got failed and explains how correctly seek over information encrypted with one-of-a-kind keys.[2] The anonymous and traceable institution facts sharing in cloud computing, on this idea the author used the idea of traceable organization statistics sharing scheme and symmetric balanced incomplete block design (SBIBD), explains a way to obtain relaxed and green information sharing in cloud environments is an pressing trouble to be solved and a way to obtain each anonymity and traceability is also a assignment in the cloud for facts sharing. A relaxed and fault-tolerant key settlement for institution information sharing in a cloud garage scheme. In taking benefit of the important thing agreement and efficient to get entry to control, the computational complexity and verbal exchange complexity for updating the common conference key. The encrypted data are quite low. [3] Fuzzy identity-primarily based facts integrity auditing for the dependable cloud garage system, using the idea of fuzzy identification-based totally virtual signature algorithm, to seek to cope with the complex key management task in cloud records integrity checking by introducing fuzzy identification-based auditing, explains about the key management in traditional far flung records integrity checking protocols and additionally provided the system and protection models for this primitive. A concrete fuzzy identification-based information integrity auditing protocol the use of the biometric-primarily based identity as an input. It also verified the security of the protocol within the selective-id model.

By the usage of the idea of identification-based totally encryption with equality check assisting flexible authorization (IBEET-FA) algorithm, [1]building IBEET-FA schemes without the use of bilinear pairing got failed and explains how correctly seek over information encrypted with one-of-a-kind keys.[2] The anonymous and traceable institution facts sharing in cloud computing, on this idea the author used the idea of traceable organization statistics sharing scheme and symmetric balanced incomplete block design (SBIBD), explains a way to obtain relaxed and green information sharing in cloud environments is an pressing trouble to be solved and a way to obtain each anonymity and traceability is also a assignment in the cloud for facts sharing. A relaxed and fault-tolerant key settlement for institution information sharing in a cloud garage scheme. In taking benefit of the important thing agreement and efficient to get entry to control, the computational complexity and verbal exchange complexity for updating the common conference key. The encrypted data are quite low. [3] Fuzzy identity-primarily based facts integrity auditing for the dependable cloud garage system, using the idea of fuzzy identification-based totally virtual signature algorithm, to seek to cope with the complex key management task in cloud records integrity checking by introducing fuzzy identification-based auditing, explains about the key management in traditional far flung records integrity checking protocols and additionally provided the system and protection models for this primitive. A concrete fuzzy identification-based information integrity auditing protocol the use of the biometric-primarily based identity as an input. It also verified the security of the protocol within the selective-id model.

[4]By means of the usage of the concept of key mixture authentication cryptosystem for records sharing in dynamic cloud storage, receives to recognize approximately the sharing encrypted statistics with different

customers via public cloud storage is a crucial studies trouble. This paper proposes a key-combination authentication cryptosystem. The statistics assaults whilst storing and sharing ought to emerge as in present-day hassle in many organizations. that is a correct idea and the number one hassle from the organizational viewpoint. this is particularly actual while trouble arises in the safety model that protects sensitive statistics and business enterprise /personal files. In the enterprise employer, the maximum critical fact loss is at the entire due to internal assaults. however, protection implemented sciences like firewalls, ids, and so forth. (already finished within the enterprise company) are very powerful. Because those strategies don't assist indoors attacks, so it can bring about reality leak problems. To check the pinnacle of a disadvantage to keep away from records leakage trouble is it what to cope with inside the route of this trouble? It's miles currently clear that the data ought to be blanketed in competition to information loss to supply an aggressive aspect. the hassle, a way to save you the facts leak, searchable technique, and having access to disadvantage whilst storing and sharing inside the cloud.[5]With the aid of the use of the concept of revocable identity-primarily based encryption technique and bilinear Diffie hellman algorithm. A likely technique to get the answer for the consumer revocation problem in IBE. On this paper, they supplied an efficient technique to the two aforementioned issues concurrently.

The dimensions of a cipher text within the cloud stays consistent, no matter how in many instances the cipher text evolves. [6] Timed-release proxy conditional re-encryption scheme(trpcre) and bilinear deffiehellman algorithm, on this author pre schemes can not assist detailed cipher textual content delegation, flexible encryption, and timed-launch delegation proposed a TRPCRE(timed-release proxy conditional re-encryption scheme) with bendy encryption for a cloud computing environment. A file proprietor is capable of authorize a cloud server to transform a designated cipher text into any other cipher text encrypted through a receiver's public key beneath a designated situation.

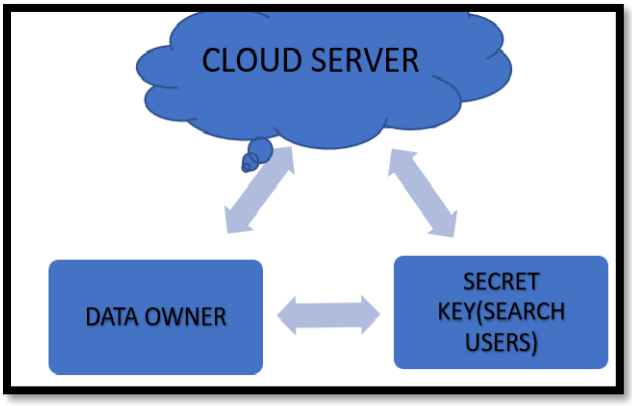


Fig4. Secret key sharing by the data owner

[7] The public-key encryption with key-word search through obfuscation, by way of using the set of rules public encryption key scheme (for key guessing assaults). The trapdoor technology technique is inefficient which might also make them inapplicable in resource-limited environments.[8]A green public-key searchable encryption scheme comfy against inside keyword guessing attacks. public encryption key scheme(for inside key guessing assaults) and dual-server public-key authenticated encryption with keyword search (DPAEKS), explains a way to seek touchy information correctly and securely. By using use of a actual-world facts set display that our scheme is especially green and affords sturdy protection, making it suitable for deployment in practical packages. [9]With the aid of the use of the concept deduplication method. CD-store is a multi-cloud garage machine for companies to outsource backup and archival garage to public cloud companies, with 3 goals in mind: reliability, security, and fee-performance.

[10] With the explosive growth of records extent, customers are increasingly inclining to store statistics at the cloud for saving local garage and computational fees. Via keeping in mind, utilization of an efficient and geometric range question scheme (EGRQ), KNN computation, polynomial fitting method, R-tree and order-retaining encryption and is the reason about with explosive increase of records quantity, users are an increasing number of inclining to save records at the cloud for saving nearby storage and computational fee. Safety analysis validated the excessive safety, confidentiality of spatial statistics, privacy protection of index and trapdoor, and the unlinkable of trapdoor. [11] Personalized search over encrypted information with green and at ease updates in mobile cloud , explains how to preserve each the privateness and value of outsourced information in cloud. By using the usage of the algorithm of

searchable symmetric encryption (SSE) and searchable public-key encryption (SPE) and personalised search scheme and ok-nearest set of rules. The comparison is performed among the customized update and search scheme & personalized seek scheme over encrypted information.

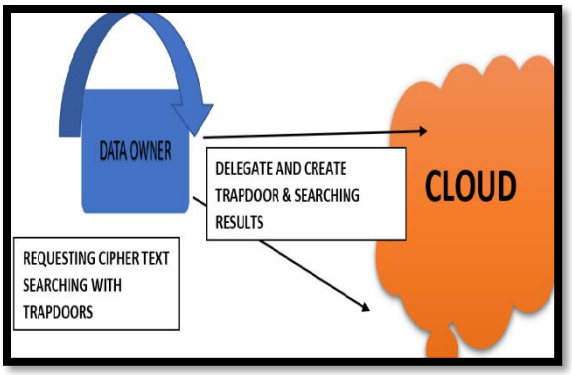


Fig5. Ciphertext Search using ABE-ET in cloud

III. KEY AGGREGATE SEARCHABLE ENCRYPTION AND DECRYPTION FOR DATA SECURE SHARED USING DIFFIE HELLMAN AND CRYPTOGRAPHY ALGORITHM

By proposing the concept of key-aggregate searchable encryption scheme and representing the concept through Diffie hellmanalgorithm and cryptographic algorithm.

A. *DIFFIE HELLMAN ALGORITHM:*Diffie Hellman's key exchange set of rules is a tightly closed manner to exchange cryptographic keys over a public conversation channel. buttons are now not exchanged - they are taken collectively. It is named after its founders Diffie and Martin Hellman. As taking reference [5] if Alice and Bob favor doing a conversation with each other, they begin to agree among themselves an oversized range of the maximum crucial p, and moreover the generator g (where 0 vary a). Therefore, shared privacy can continuously be similar. In ephemeral-static mode, one crew can generate a replacement non-public/public key frequently, consequently a substitute shared mystery is going to be created.

B. CRYPTOGRAPHIC ALGORITHM:

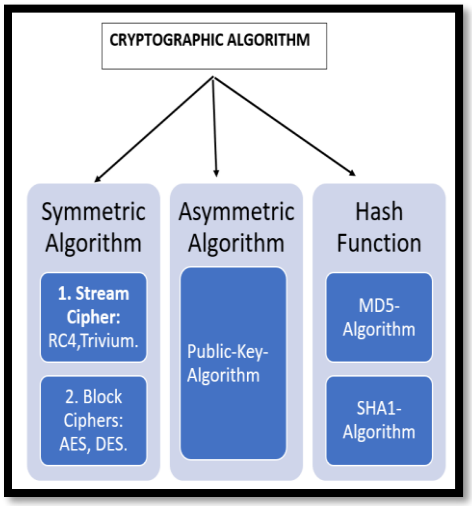


Fig6. Cryptography algorithm types

The cryptologic protection of the system in competition to attacks and malicious penetration is predicated on two parameters: (1) the energy of the keys and therefore the effectiveness of the mechanisms and protocols associated with the keys; (2) And keys secured via key management (storage, distribution, use, and destruction). strong algorithms blended with susceptible key administration square measure seemingly to fail the inclined algorithms embedded in the context of sturdy key control.

a. SYMMETRIC ALGORITHM:

Additionally, called a secret-key method, the symmetric-key system converts statistics to structure it very hard to check whilst not having a secret key. The secret's idea of symmetrical as a stop result of it's miles used for each encrypting and decrypting. Those keys are on occasion proverbial with the aid of 1 or greater authorized corporations. the secret's notion of symmetrical as a cease result of it's far used for each encrypting and decrypting. Those keys are now and again proverbial through one or more authorized firms.

Symmetric key algorithms are used for:

1. Offer information confidentiality using the equal key to encrypt and decrypt facts.

2. Provide message authentication codes (macs) for useful aid and integrity authentication offerings. The secret's used to create a mac after which validate it.

3. Installing keys at some point of key-set up tactics

4. Generate preventive random numbers.

b. ASYMMETRIC ALGORITHM:

Additionally known as public-key algorithms, secret key algorithms use paired keys (public and personal keys) to function their operation. The typical public key is provided to all or any, but, the private key is controlled entirely with the aid of way of the proprietor of that key mixture. Private key counts can't be calculated with the aid of victimization public keys and they're cryptographically linked.

Asymmetric algorithms are used for:

1. Counting digital signatures.

2. Status of cryptographic function.

3. Identity management.

c. HASH FUNCTION:

The scientific self-discipline hash operate does not use keys in its fundamental practicality. This overall performance creates little grinding or "hash value" from large quantities of facts in an rather unidirectional method. The hash function is generally accustomed construct constructing blocks utilized in key administration and to produce protection offerings such as:

1. Provide authentication assets and sources via growing Message Verification Codes (MACs).
2. Press messages to create and affirm digital signatures
3. Cut the buds into the enter key algorithms
4. Create random block numbers

First, statistics proprietor totally has to distribute one combination key to a consumer for sharing any range of files. Second, the person entirely has to put up a single combination trapdoor to the cloud for play acting keyword search over any range of shared files. Modules rectangular measure about to cowl proven below:

a) Key generation: For the duration of this module, the admin is going to come up with keys for mystery writing and the cryptography method. By means of a victimization choppy system, the admin goes to provide you with the draw close and public key.

b) Get admission to manage: During this module, the admin is going to grant get right of access to administration for the files that the facts owner is going to exchange whereas the importing admin is going to encode the document with the help of the hold close mystery key for the safety reason of the cloud.

c) Key-word indexing: Throughout this segment, it eliminates spare phrases from the record and realizes the important thing phrases of the files/information. And so we can calculate the content weightage of key phrases convert the key terms into hash code through victimization MD-5algorithm and region the hash code inside the index array.

d) Send aggregate key: To be supported the schooling chosen through way of the admin, the device ought to fetch the corresponding hash keys and fetching the hooked up public key. It will generate the person mixture key and ultimately ship it to the legal user.

e) Seek with keyword: The individual must select the combination key then in a while input the hunt keywords. Convert the key-phrase into hash code. Thereupon it'll decode the combination key. Separates and receives the hash key and public key. Victimization hash key and key-word generate trapdoor (hash code). By means of causation, the trapdoor to the server, supported the trapdoor received the trapdoor via the server need to check the important thing-phrase index and if any matching records rectangular degree supplied listing all of the filenames to the person. (regulate and inform) examine the shortlisted files from the server, transfer the archives and in the long run rewrite the files with the statistics proprietor public key.

IV. METHODOLOGY

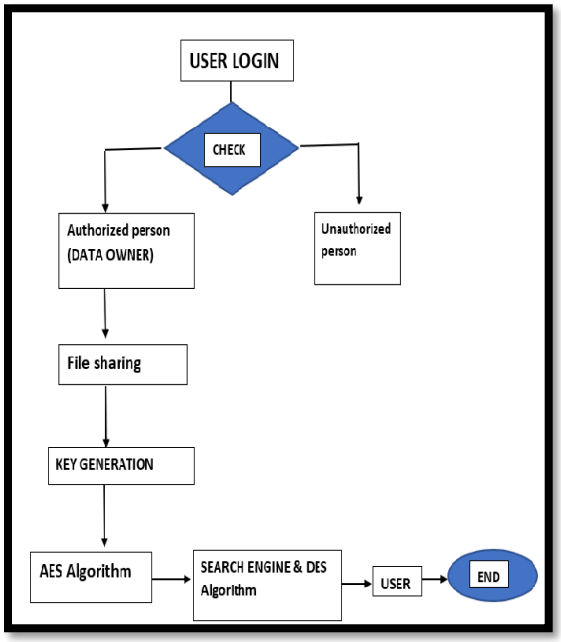


Fig 6. System flowchart

a) The need to first share encrypted data sincerely top notch in some of in numerous methods that normally want great secret writing keys that vicinity gadgets used for various records or documents. But, the extent of keys that has obtained to be distributed to a couple of customer to seem for encrypted documents and delete encrypted files is enough for the quantity of those files. Such an outsized extent of keys are now not absolutely dispensed to customers via impervious channels as an alternative moreover are firmly keep and maintained thru clients on their gadgets. In addition, customers want to produce an outsized variety of loops and ship them to the cloud to characteristic keyword searches on a couple of files. Exploitation key mixture secret writing (KASE) strategies, the AES algorithmic rule is hired to interchange a file to the cloud.

b) The AES set of rules generates a public key and a non-public key the usage of the important thing private key to add a document. With the help of the public key and the hash key, the merge key is created; trapdoor keyword: the DES set of rules is used to encrypt the united states key for protection features and is based totally on the rating set of rules, widely recognized key phrases are stored and real cloud garage: second, an

integrated trapdoor need to be moved within the cloud by way of person searches. The key-phrase above cloud facts sharing and cloud records protection as tested in the discerning above is the amount of the shared document, the approach of formulating how it works, and its approach as validated in device layout.

Techniques are defined in important points below:

Strategies are defined in essential factors below:

a) Admin set of rules: For placing up a separate plan, the commonplace parameters of the device are generated with the resource of the cloud server setup algorithm, and those accessible parameters may be reused to percentage their statistics with one-of-a-kind information owners.

b) Generate a set of rules: For the period of this module, the admin planning to generate keys for cryptography and the name of the game writing approach. with the aid of mistreatment choppy algorithmic rule, admin making plans to generate a keep close mystery key and public key. For each and each facts proprietor, he/she need to supply a public / grasp-secret key try.

c) Searchable cryptography algorithm: The keywords of each and every file/record are frequently encrypted and if the consumer desires to seem for the data set with the aid of the owner of the file mistreatment searchable cryptography topic.

d) Get entry to the administration set of rules: During this module admin making plans to grant get right entry to administration for the data he/she can make plans to transfer, while the uploading admin planning to cipher the file with the help of the maintain close secret key for the safety purpose of the cloud.

e) Calculation of key-word set of rules: For keyword compartmentalization, disposing of supernumerary phrases from the record, and recognize the keywords. Calculate the content weightage of key phrases converts the keywords into hash code thru mistreatment MD-5 algorithmic rule, the neighborhood the hash code in index array.

f) Send an aggregate key set of rules: Supported the suggestions parent out on with the useful resource of admin, the machine wants to fetch the corresponding hash keys + fetch the normal public key. Generate the user aggregate key and at closing, deliver it to users.

g) Secret writing (seek with keyword) set of rules: User wants to select out the combination key then at that point enter the search keyword. Convert the key-word into hash code. decipher the mixture key, separate and find out hash keys and separate and discover the public key. Mistreatment hash key and key-phrase generate hash codes (trapdoor).

h) Modify algorithm: Send the hash codes to the server, supported the hash codes obtained server ought to take a look at the key-phrase index and if any matching documents location unit provided, list all of the report names to the consumer. (Adjust & check) Take a look at the shortlisted information from the server, alternate the documents, and at remaining to decipher the file with the proprietor's public key.

V. SYSTEM DESIGN

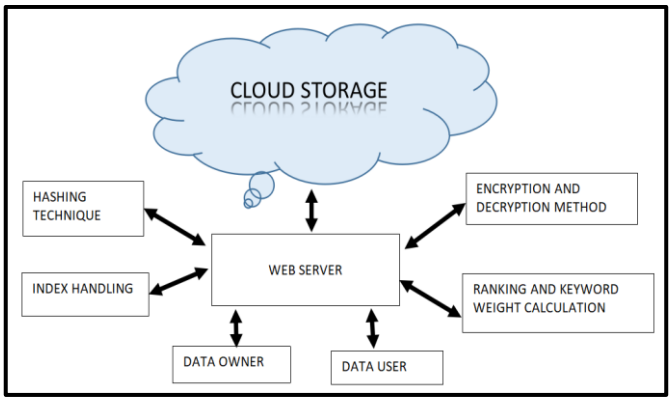


Fig 7. System Architecture

Fig7 tells us about how the data is stored in the cloud and the process of data sharing protection through encryption and decryption and search keywords by calculating keywords to make user access to his or her documents by data owner through hashing and index management. Basic Techniques /Algorithms used:

a) Hashing algorithm: This algorithm gives a method that permits records proprietors to affix to encrypt records such that the user can experiment with the QR code and decrypts the statistics.

b) Index Handling: Indexes vicinity unit accustomed hastily discover records while now not having to appear to be every row in a very information table every time a statistics table is accessed and might additionally be dealt with nicely.

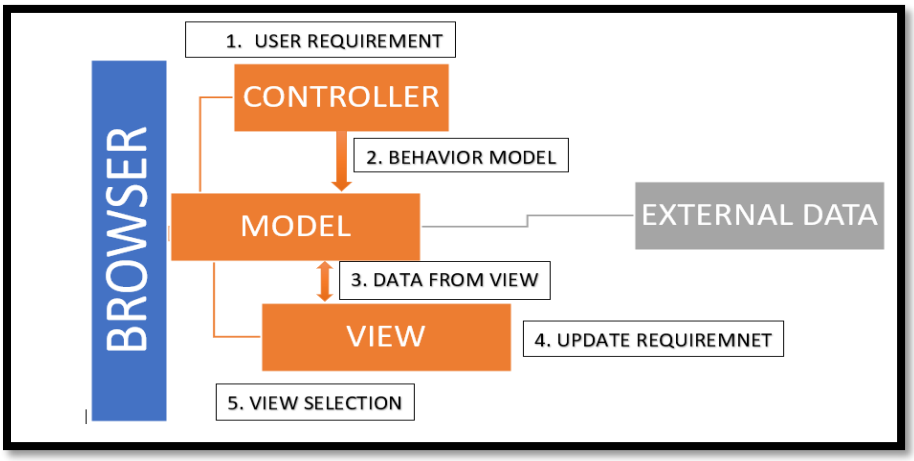
c) Encryption & Decryption Algorithm: AES Algorithm (Advanced Encryption Standard Algorithm): AES set of rules is used to extend records safety and confidentiality. The operating principle of the AES algorithm is to work thru taking the simple text and convert the undeniable text into ciphertext, that's normal of curiously random characters. Completely those who have the name of the game key will decode it. As a end result of it makes use of radially symmetrical key mystery writing, which involves using the totally secret key to ciphertext and deciphers text statistics. By way of explaining the usage of the AES algorithm, we acquired to apprehend approximately the AES set of rules also can be called a cryptographic algorithm used to guard the statistics. It's miles a radial block ciphertext that may additionally encipher and decipher the statistics (records dispatched through the records owner) and authorized consumer.

i. Encryption: This scheme converts the records to a shape known as ciphertext.

ii. Decryption: This scheme converts the facts decrease again into its particular form called undeniable textual content.

2. DES Algorithm (Data Encryption Standard Algorithm): DES algorithm is used to take the simple textual content in sixty-four-bit blocks & convert them into the ciphertext using 48-bit keys. The running principle of the DES algorithmic software program is to figure by way of manner of encrypting agencies of sixty-four message bits, which is identical to sixteen positional example tool varieties. If the ciphertext is decrypted with the important thing des key and we can see the genuine simple text. by way of explaining the des algorithmic software usage, must be compelled to apprehend that it is a block cipher algorithmic software that takes the simple textual content in blocks of sixty-four-bits and converts them to ciphertext victimization keys of 48-bits. It's miles a bilateral key algorithmic software that shows that an equal secret's used for secret writing and decoding understanding.

d) Ranking Algorithm and weight calculation: A scoring algorithm is getting used to weigh the range of things to decide which webpage is the most blanketed and secured and moreover applicable to a search query in a seek engine. As inside the weight calculation of the web page, when the information proprietor sends a giant form of pages within the cloud, the character faces the problems in searching which statistics is being dispatched via the owner, which potential for identification of precise facts deliver by using the usage of the proprietor to the certified consumer. So according to that, even a unique web web page is related with specific pages that are taken as important pages and moreover along with that it's going to calculate the internet page weight rank which is going to make individual ease in looking out the files, documents, and many others.



VI. IMPLEMENTATION

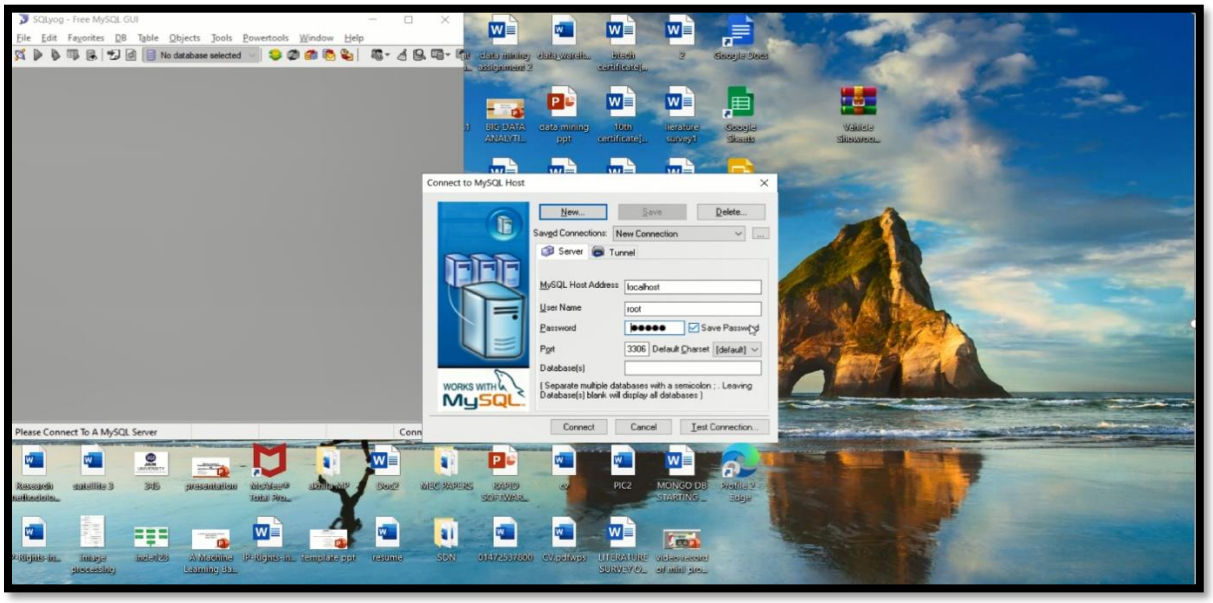


Fig 6.1 Connection between the MYSQL and SQLYog

Fig 6.1 illustrates the connection between the MYSQL and SQLYog in which they asks for the username and password for get connected to the SQLyog for getting the information about the user details whether they are insider/outsider malicious to know and along with the uploaded files details and to identify the files are correct or wrong and it also tells about the the behaviour who had logged in the web application, here they identifies the behaviour of user.

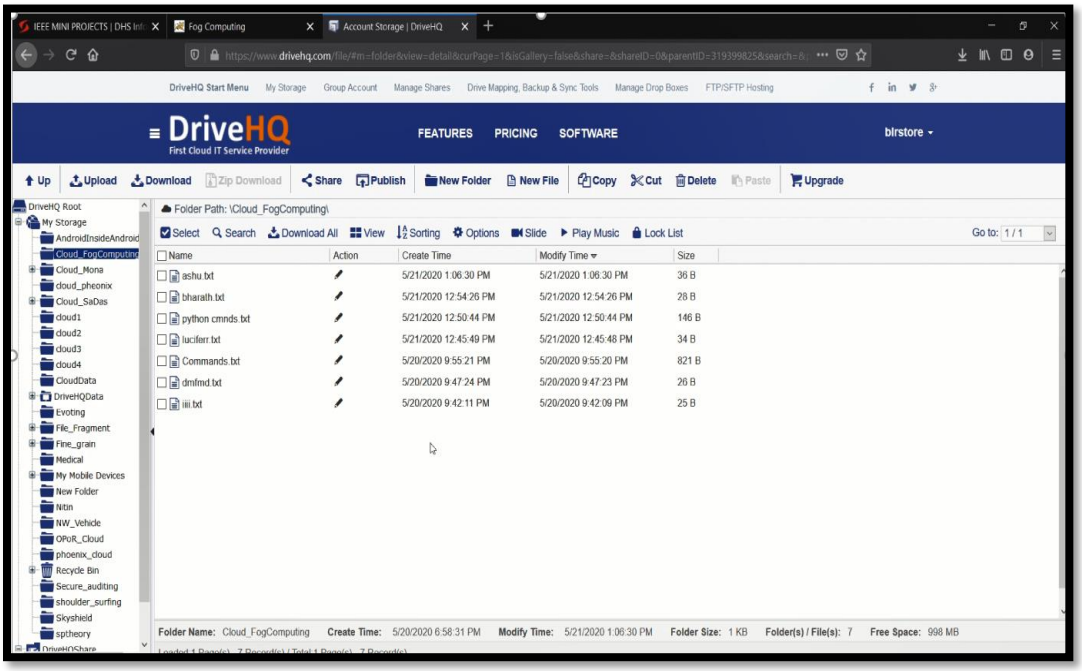


Fig 6.2 Uploaded files in the cloud

Fig 6.2 illustrates the files which are uploaded in the web application they gets stored in the cloud service provider along with the date and time and the size of the file which they are already connected with the Tomcat web application manager.

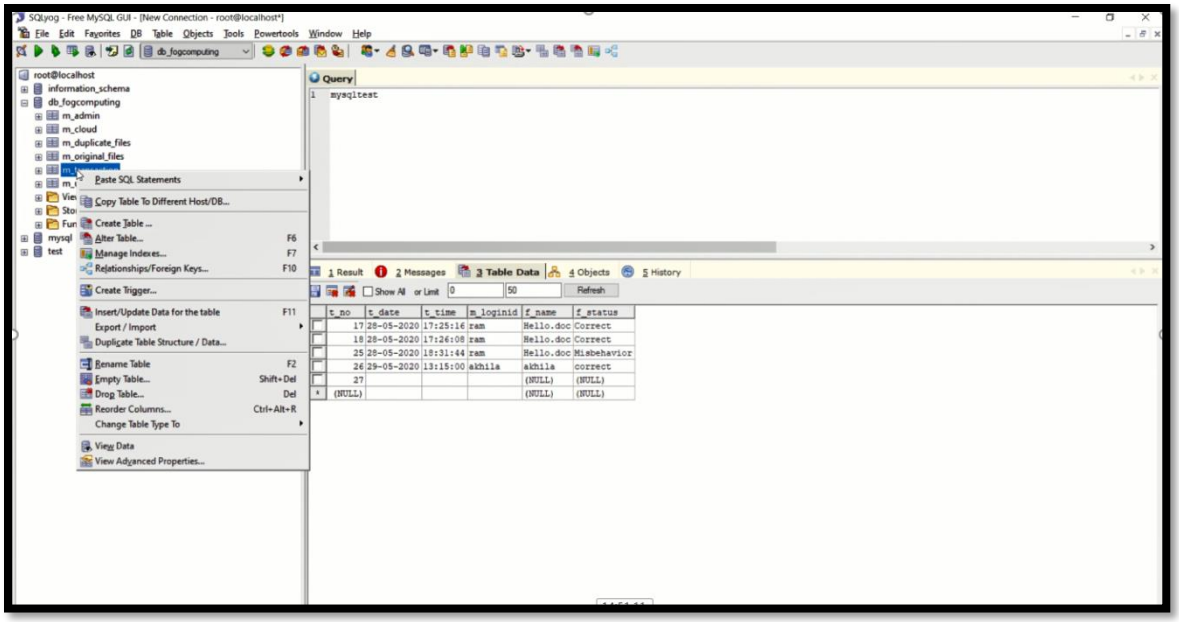


Fig 6.3 Detailed information with time and date

Fig 6.3illustrates detailed information of each user with time and date and also about the uploaded files in the SQL with the detailed information like behaviour of the user whether they did misbehave or behave properly, date of the uploaded files by the user, time of the uploaded files by the users, along with the uploaded files with null notes inside them, etc.

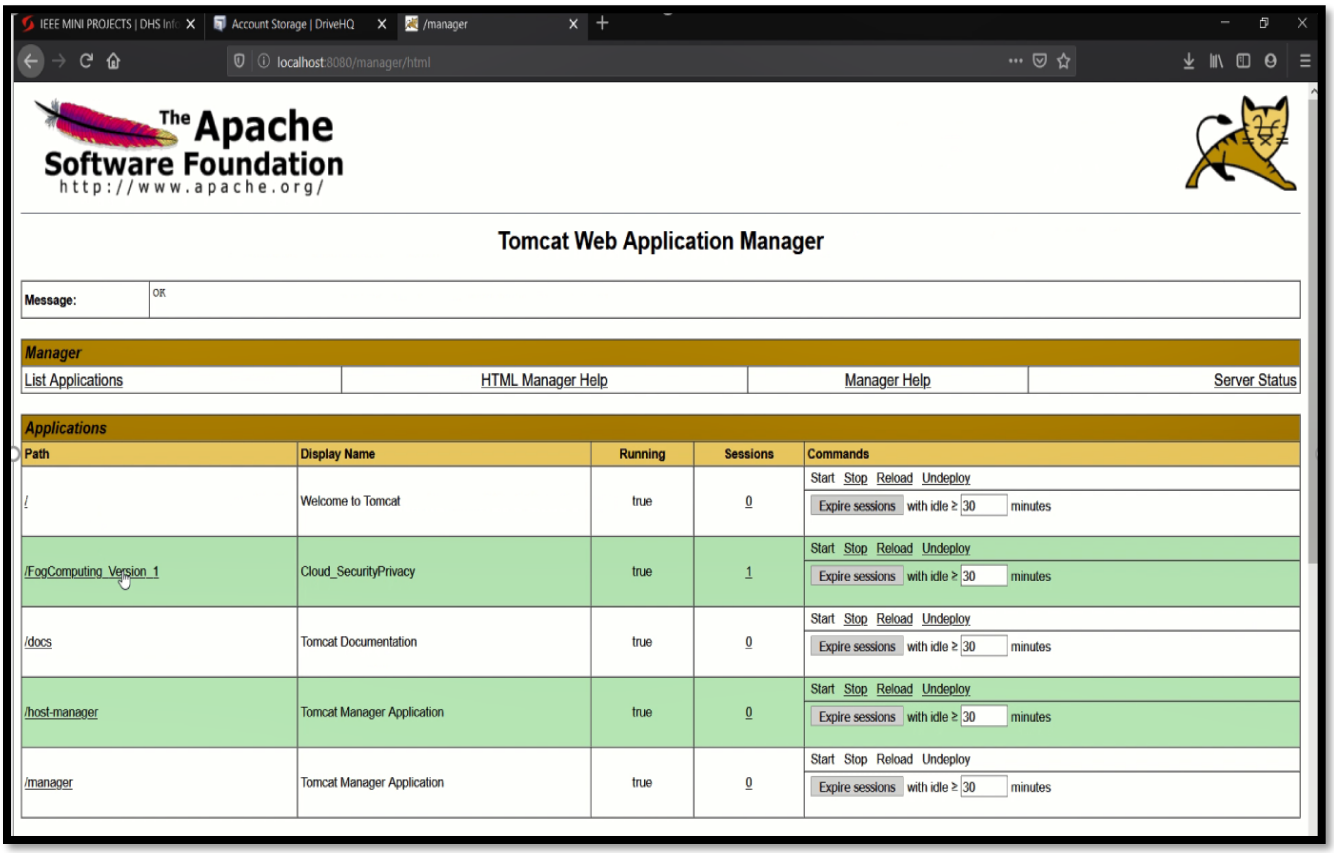


Fig 6.4 Connection of Tomcat Application Manager

Fig 6.4illustrates connection of tomcat application manager in this figure they tells the connection is done when the MYSQL and SQLyog gets connected to each other to create the user profile and get the entry in the web application called Tomcat application manager.

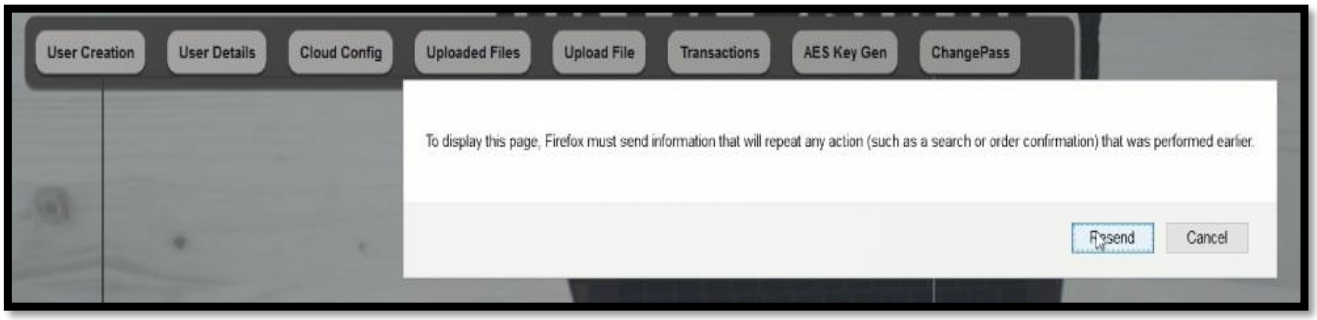


Fig 6.5 Master Key Generation and Change Password

Fig 6.5illustrates about the master key generation and changing the password and along with that they tells about the user can change the password after uploading your files/documents in which, when the user clicks on the secret key which is used for encrypting the files which are already uploaded.

VII. CONCLUSION

The necessary function of the important thing mixture searchable encryption and decryption scheme is to guard the sensitive data and making the secret key for the facts owner for encrypting the facts and decrypting the statistics for the licensed user through manner of the utilization of the decryption method for decryption the secret key. The important trouble may be passed off to retain the get admission to control and to advocate the exquisite reply for the economic agency troubles and issues. This paper proposed the key aggregate encryption and decryption-primarily based cryptography set of rules for cloud issuer vendors' encryption and decryption give up pointing mechanism to reduce the above-cited problems; It additionally explains the encryption and decryption strategies, usages, and their running ideas. And it moreover explains how the encryption and decryption techniques may be extended in getting admission to manipulating within the cloud and seeking out encryption in cloud-based totally statistics safety as confirmed from the device graph according to the techniques used for it

VIII. REFERENCES

[1] S. Ma, Q. Huang, M. Zhang, and B. Yang, "Efficient public-key encryption with equality test supporting flexible authorization", *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 458-470, Mar. 2015.

[2] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems", *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 1, pp. 72-83, Jan./Feb. 2019.

[3] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage", *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 127-138, Mar. 2015.

[4] H. Zhu, L. Wang, H. Ahmad, and X. Niu, "Key-policy attribute-based encryption with equality test in cloud computing", *IEEE Access*, vol. 5, pp. 20428-20439, 2017.

[5] Q. Wang, L. Peng, H. Xiong, J. Sun and Z. Qin, "Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing", *IEEE Access*, vol. 6, pp. 760-771, 2018.

[6] Q. Wang, L. Peng, H. Xiong, J. Sun and Z. Qin, "Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing", *IEEE Access*, vol. 6, pp. 760-771, 2018.

[7] Y.-M. Tseng, T.-T. Tsai, S.-S. Huang and C.-P. Huang, "Identity-based encryption with cloud revocation authority and its applications", *IEEE Trans. Cloud Comput.,2016.*

[8] Y. Sun, F. Zhang, L. Shen, and R. H. Deng, "Efficient revocable encryption against decryption key exposure", *IEEE Inf. Secure.*, vol. 9, no. 3, pp. 158-166, 2017.

[9] S. Park, K. Lee and D. H. Lee, "New constructions of revocable identity-based encryption from multilinear maps", *IEEE Trans. Inform. Forensics Security*, vol. 10, no. 8, pp. 1564-1577, Aug. 2015.

[10] Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing", *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 425-437, Feb. 2019.

[11] Li, Y. Shi, and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage", *IEEE Int. J. Commun. Syst.*, 2018.