Multi-Owner Keyword Search Over Cloud with Cryptography

Shaikh Rohan Ali[1], Javed Md. Khan [2], Chaudhari Khuduspasha [3], Mr. Shaikh Sharique Ahmad[4]

[1,2,3]B.E. (Computer) Pursuing Jamia Institute of Engineering & Mgmt. Studies, Akkalkuwa, Maharashtra India
[4]M.E. (Computer), Lecturer Jamia Institute of Engineering & Mgmt. Studies, Akkalkuwa, Maharashtra India

***

Abstract - *In first, most of the prevailing schemes most effective bears in thoughts the state of affairs with the single data owner. 2nd, they need at ease channels to guarantee the relaxed transmission of thriller keys from the records owner to statistics customers. 0.33, in a few schemes, the statistics owner needs to be online to assist facts customers at the same time as data clients intend to perform the search, this is inconvenient. Searchable encryption lets in cloud customers to outsource the huge encrypted statistics to the along way-flung cloud and to go looking over the information without revealing the touchy information. Many schemes have been proposed to resource the important thing-word seek in a public cloud. But, they have got a few ability limitations. To enable users to quickly type out the records of pastimes from massive encrypted facts, searchable encryption has been proposed and enriched by way of many schemes. rather than decrypting the complete information, those schemes allow users to appearance over the encrypted facts and pleasant decrypt the corresponding files. Searchable encryption schemes were proposed to clear up the problems caused at the same time as the information proprietor shares the statistics with a couple of customers*

Keywords—component, formatting, style, styling, insert (key words)

1. INTRODUCTION

The short growth of cloud customers has affirmed that cloud storage services are becoming the inseparable part of humans' life. Customers can experience a greater reachable and price-green storage environment than preserving a local storage infrastructure. However, the reality that cloud garage offerings offer massive convenience for customers, statistics confidentiality and privacy is probably placed at danger even as clients outsource the facts to a miles-flung cloud server. Clearly, encrypting the information earlier than outsourcing is a way to defend facts privateers. However, this may make facts utilization, collectively with keyword search, a completely hard project [1]. Those schemes permit customers to search around over the encrypted records and handiest decrypt the corresponding documents. Maximum of the prevailing schemes simplest takes into account the state of affairs of a single facts proprietor. As opposed to handiest one records owner, most cloud companies, in truth, serve a couple of statistics owners who are able to percentage their information with every different. For the reason that data sharing is turning into increasingly important at the user facet, the way to permit facts customers speedy and securely discover the information of interests from a couple of information owners' facts will become hard trouble. Due to the huge transmissions of secret keys, it isn't reasonable to without delay enlarge the present schemes from one statistics proprietor to multiple data owners.

1.1 What is multi owner keyword search over shared data?

The information is significant information' raw fabric. The information shared via the use of the cloud computing concept. The key-word is a component which to go looking on the basis of client's quires. [14] In shared facts, all vital records available thru simply. The person that can be looking the information to get right of access to virtual information its dealt with as a "multi-proprietor". At the back of the concept of the unmarried owner, it deals with more than one key-word searching procedures. [1]. specific facts objects (or documents, we do no longer distinguish the belief of facts with that of the record within the course of the paper as international locations are interactively used in masses of references mentioned right here) outsourced are encrypted by means of a single key. [2-9] the statistics retrieval line of work and the oblivious switch line of labor fall on this magnificence. Most of the research on searchable encryptions centered on the case whilst data are encrypted with the identical key and extra green solutions have been proposed in current years. The idea behind the ones buildings is that to access a database, in my opinion authorized consumer is issued a question key by using the information owner and simplest the legal clients who've valid query keys can generate legitimate get proper of access to queries which allow the database manipulate server to procedure users' are seeking for queries without gaining knowledge of the keywords contained within the queries and the contents of the encrypted statistics.

1.2 Impaction of cloud computing on multi owner keyword search over shared data

The records of visitors need to be extended due to the expandability of the internet of factors. In today's generation server have a tremendous impact on the facts manipulate. In the back of the idea of man or woman servers, we difficulty this period with allotted server fashion. The speedy growth of cloud customers has affirmed that cloud storage offerings are getting the inseparable a part of human beings' lifestyles. Users can enjoy an extra on hand and price-green garage surroundings than keeping a neighbourhood storage infrastructure. No matter the reality that cloud garage services offer large comfort for customer's records confidentiality and privacy might be positioned at threat while clients outsource the records to a mile off cloud server. Certainly, encrypting the data earlier than outsourcing is an approach to defend facts privateers. But, this may make facts usage, which includes key-phrase search, a very hard task. [6], [7]

Cloud computing protection is a brief-growing carrier that offers the numerous same functionalities as traditional IT safety. This includes protective important statistics from robbery, records leakage, and deletion. One of the blessings of cloud offerings is that you can feature at scale and although continue to be comfy. It is similar to how you presently manipulate safety, however now you've got new strategies of turning in protection solutions that address new regions of the mission. Cloud protection does not exchange the method on a manner to manipulate safety from stopping to detective and corrective actions. But, it does, however, give you the capability to carry out those activities in an additional agile manner

Your information is secured inside statistics centres and wherein some nations require facts to be saved in their united states, selecting an issue that has multiple records centres internationally can help to read this. Statistics storage regularly includes sure compliance requirements, especially while storing credit rating card numbers or health information. Many cloud companies provide impartial zero.33-celebration audit reviews to attest that their inner system exists and are effective in coping with the security inside their centres in which you keep your information. [17].

2. PROBLEM DEFINATION

In first, the vast majority of the current plans just think about the situation with the single information proprietor. Second, they need secure channels to ensure the protected transmission of mystery keys from the information proprietor to information clients. Third, in certain plans, the information proprietor ought to be online to help inform clients when information clients expect to play out the hunt, which is badly arranged. Accessible encryption permits cloud clients to re-appropriate the monstrous scrambled information to the remote cloud and to look over the information without uncovering the touchy data. Numerous plans have been proposed to help the watchword seek in an open cloud. In any case, they have some potential confinements. To empower clients to rapidly deal with the data of premiums from expansive scrambled information, accessible encryption has been proposed and enhanced by numerous plans. Rather than decoding the entire information, these plans enable clients to look over the scrambled information and just unscramble the comparing records. Accessible encryption plans have been proposed to tackle the issues caused when the information proprietor imparts the information to numerous clients. [2-9]

3. LITERATURE SURVEY

Due to the fact that music et al. [2] supplied the primary sensible searchable encryption scheme, many observe-up schemes have been proposed in the literature [3,4,20-22]. Some of these schemes only permit the facts owner to search over the encrypted statistics, which aren't inappropriate for statistics sharing offerings inside the cloud. In mild of this trouble, some schemes [5-9,19] were proposed to support multi-consumer searchable encryption, implying that the facts can also be searched by using authorized customers thinking about the cost of building the secure channels, Beak et al. [10] proposed the first scheme, called secure channel free searchable encryption (SCFPEKS), aiming to dispose of the relaxed channels from searchable encryption. Rhee at al. [11] delivered an enhanced security version and constructed a scheme on this model. To improve performance, GU et al. [12] presented a unique SCF-PEKS scheme without pairing operation Rhee at al. [11] brought a superior security version and constructed a scheme on this model. To enhance performance, GU et al. [12] supplied a unique SCF-PEKS scheme without pairing operation.

If there are many information proprietors who are inclined to share their information with each other, new searchable encryption is required. For the answers with comfortable channels, every information owner has to establish an at ease channel with a records person and transmits the secret records via the channel. It way that each the computation overhead and conversation overhead growth with the wide variety of facts owners. For the SCF-PEKS schemes, each records proprietor has to encrypt every key-word for each statistics user. The computation overhead and garage overhead will growth no longer handiest with the variety of facts users however also with the variety of keywords. Consequently, it's miles great to layout searchable encryption without comfy channels in a multi-owner placing.

4. EXISTING METHODOLOGY

Inside the present system, the maximum of the prevailing schemes most effective keep in mind the situation of a single records owner. as opposed to most effective one information proprietor, maximum cloud carriers, in fact, serve a couple of statistics owners who are capable of proportion their records with each different. Since the records sharing is becoming increasingly more critical at the user aspect, how to let records customers fast and securely find out the facts of pastimes from more than one data proprietors' facts turns into a difficult problem. Because of the big transmissions of mystery keys, it isn't always reasonable to at once expand the existing schemes from one facts owner to a couple of information proprietors. [18]

A. System model

The machine version includes 3 entities the manager, users, and the cloud server. The supervisor takes charge of the institution management, consisting of adding a new consumer and doing away with a revoked user. Each user within the institution is taken into consideration as a licensed person, which means that the user concurrently performs roles: an information proprietor and a facts user. As a statistics owner, the person can share his encrypted information with other legal customers within the group. And as a facts person, the consumer can search over the encrypted facts of others in the organization. After the manager allows a new consumer to join the organization, the brand new person desires to add the general public key to the cloud server. Then the manager publishes a notification to the cloud server, which informs each legal consumer to download the public key of the new person and generate a re-encryption key for the new consumer. After that, the brand new person can enjoy searching over the encrypted information of others in the group. Analogously, to permit the legal customers to search over the information of the new consumer, this new user desires to generate a re-encryption key for each authorized user and uploads these keys to the cloud server. To revoke a user from the group, the manager simplest wishes to request the cloud server to delete all the re-encryption keys related to the revoked user. Since our scheme makes used.

B. Security model

In this work, we recollect that there is no secure channel in our machine. All of the records transmitted can be intercepted by means of a choosadversary who can listen in on transmission channels.

It method that no secret facts are permitted to be transmitted through transmission channels. Meanwhile, we recall the honest but curious cloud server like the maximum of the prevailing works. The cloud server will simply observe our proposed protocol, however curiously try to research as a great deal additional records as viable from the acquired information. It's miles well worth noting that we forget about the collusion among the cloud server and revoked customers. In addition, no legal user will help the cloud server find out additional records. Moreover, the cloud server will now not assist revoked users to preserve the privilege which they ever owned inside the group.

C. Design objectives

Our scheme ambitions to attain subsequent goals.

1. **Safety: -** Even in the environment without at ease channels, our scheme should nevertheless save you the cloud server from getting to know extra statistics and keep the contents of the documents, the keywords within the index, and the key-word in trapdoors as secret.

2. **Efficiency: -** Our scheme ought to reap an appropriate performance from a person's angle.

3. **Efficient person Adjustment: -** Our scheme has to guarantee that the consumer adjustment is green and relaxed. Only the legal users can perform the hunt over the encrypted statistics shared within the group. The revoked users will lose the privilege of the hunt.

5. PROPOSED METHODOLOGY

In first, the maximum of the prevailing schemes best recalls the state of affairs with the single information owner. Second, they want comfortable channels to assure the cozy transmission of secret keys from the statistics owner to facts users. 1/3, in some schemes, the records proprietor ought to be online to assist records customers while facts users intend to perform the hunt, that is inconvenient. Searchable encryption permits cloud customers to outsource the huge encrypted facts to the far off cloud and to go looking over the data without revealing the touchy records. Many schemes have been proposed to guide the key-word seek in a public cloud. But, they have a few capacity obstacles. To enable users to speedy kind out the statistics of interests from huge encrypted records, searchable encryption has been proposed and enriched through many schemes. In preference to decrypting the complete records, these schemes allow users to look over the encrypted information and best decrypt the corresponding files. Searchable encryption schemes were proposed to solve the troubles brought on while the facts proprietor shares the facts with a couple of users. [2-9]. We advise a novel searchable scheme which helps the multi-owner keyword seek without at ease channels. Greater than that, our scheme is a non-interactive solution, wherein all the customers handiest need to talk with the cloud server. Moreover, the analysis proves that our scheme can assure safety even without secure channels. Not like maximum existing public key encryption primarily based searchable schemes, we evaluate the performance of our scheme, which suggests that our scheme is sensible. We provide secure and privacy-maintaining access manipulate to customers, which guarantees any member inside the organization to anonymously utilize the cloud aid. Furthermore, the real identities of statistics owners can be discovered through the group manager when disputes occur. Right here we use than the variety of servers and at the back of the concept of centralized. We concentrate on some convenience

1. Timing intake is less

2. Decryption key should be sent via a secure channel and kept secret.

3. It is an efficient public key encryption scheme which supports flexible delegation.

So these aspects stand as a tool for reduce power of internet scale in the steganography.

6. ARCHITECTURE

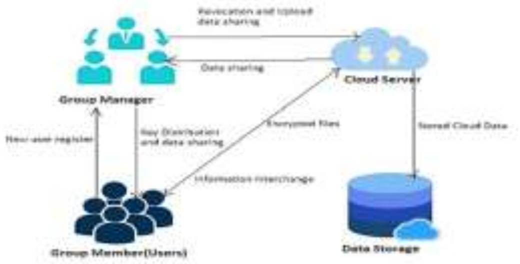


Fig -1: Architecture of System

MODULE DESCRIPTION

It consists of 4 modules which to be specified here,

1. Group Manager Module
2. Group Member Module
3. Cloud Module
4. User Module

Group Manager Module

a) In our scheme, we do not forget that the supervisor is an initiator who creates a collection.

b) The manager takes a fee of the group control, including a brand new person and removing a revoked consumer.

c) Every person within the group is taken into consideration as a certified person, because of this that the consumer simultaneously performs two roles: a records proprietor and a statistics consumer. As facts proprietor, the consumer can percentage his encrypted facts with different legal customers in the institution.

Group Member Module

a) As a data user, the person can seek over the encrypted information of others inside the group. After the manager allows a new consumer to enroll in the institution, the new person desires to add the public key to the cloud server.

b) Then the manager publishes a notification to the cloud server, which informs every authorized person to download the public key of the new user and generate a re-encryption key for the brand new person.

c) After that, the new user can revel in searching over the encrypted facts of others within the group.

Cloud Module

a) The rapid growth of cloud users has Affirmed that cloud storage services have become the indivisible a part of people's life.

b) Despite the removal of secure channels, these solutions are still aloof from being deployed in an exceedingly real public cloud. Most cloud suppliers, in reality, serve multiple knowledge homeowners WHO are ready to share their data with one another.

c) The cryptographic primitive known as proxy re-encryption is employed to assist knowledge owners delegate the power of search to data users via the cloud server, while not revealing any extra info.

User Module

a) User revocation is performed by the cluster manager via a public obtainable revocation list (RL), supported that cluster members will inscribe their knowledge files and make sure the confidentiality.

7. DIAGRAME

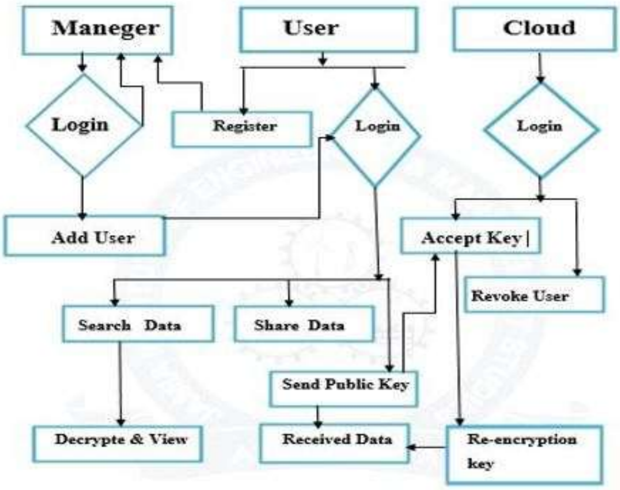


Fig -2: DFD (Data Flow Diagram)

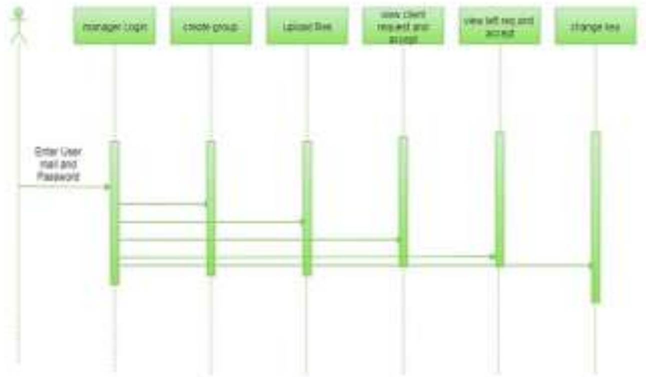


Fig -3: Sequence diagram of Manager module

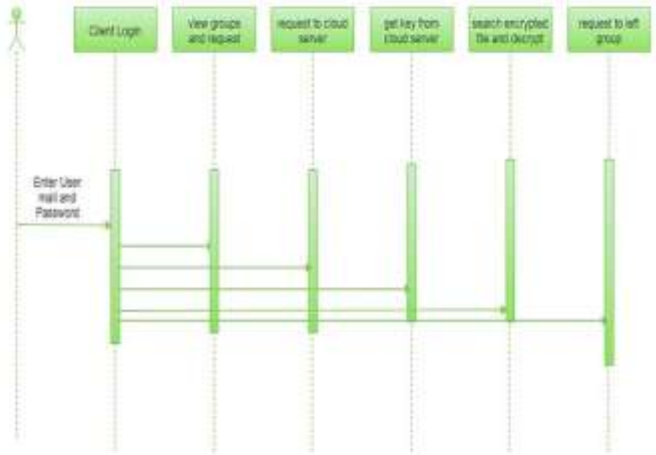

Client Login
View groups and request
request to cloud server
get key from cloud server
search encrypted file and decrypt
request to left group
Enter User mail and Password

Fig -4: Sequence diagram of Data User module

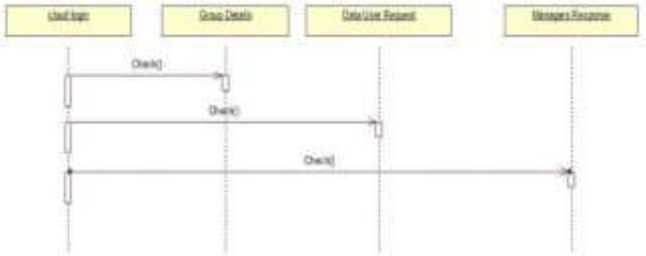


Fig -5: Sequence diagram of Cloud module

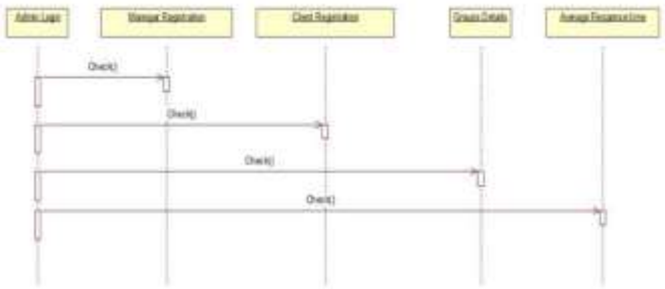


Fig -6: Sequence diagram of Admin module

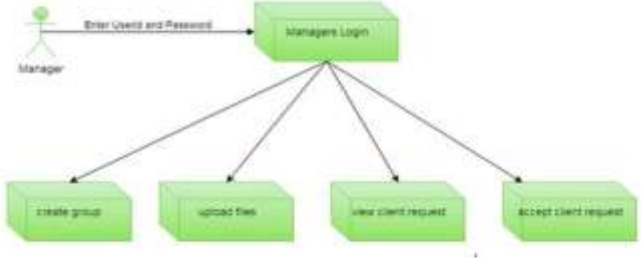


Fig -7: Components diagram of Manager Panel

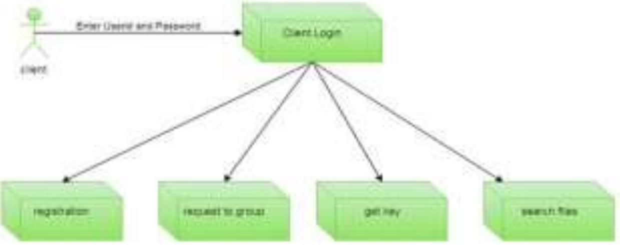


Fig -8: Component Diagram of Data User Panel

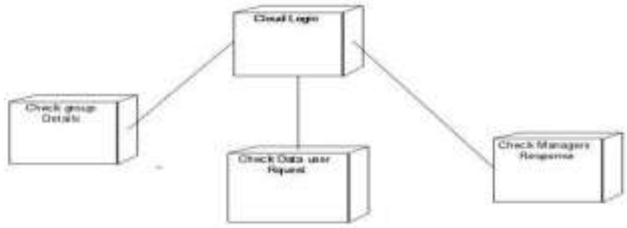


Fig -9: Component Diagram of Cloud Panel

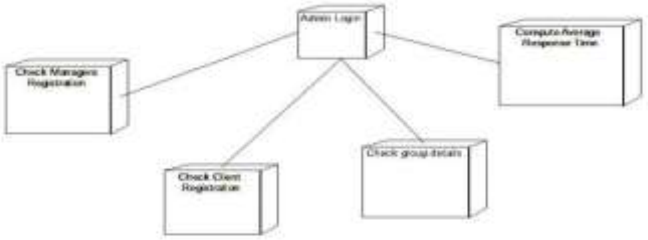

Admin Login
Check Managers Registration
Compute Average Response Time
Check Client Registration
Check group details

Fig -10: Component Diagram of Admin Panel

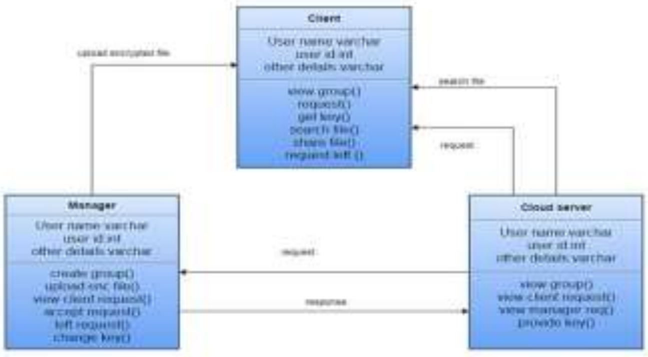


Fig -11: Class Diagram of the project

8. DIAGRAME

1. **SKE.Gen (1k) →K:** Inputs a security parameter 1k, the key generation algorithm SKE. Gen outputs a key K.

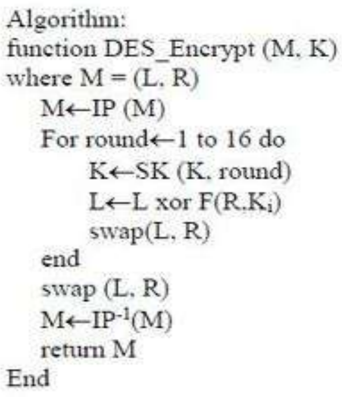
2. **SKE.Enc (K, m) →c:** Inputs a key K and a message m, the encryption algorithm SKE.Enc outputs a cipher text.

3. **SKE.Dec (K, c) →m:** Inputs a key K and a cipher text c, the decryption algorithm SKE.Dec outputs a message.

Many businesses and those store their crucial statistics on cloud and information is also accessed through many folks, so it's far very crucial to relaxed the facts from intruders. To provide safety to cloud many algorithms are designed. A few popular algorithms are

A. Data Encryption Standard (DES)

This stands for data Encryption standard and it changed into advanced in 1977. It becomes the first encryption trendy to be recommended by means of NIST (National Institute of standards and technology). DES is 64 bits' key length with 64 bits block size. Considering that that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher. [23]



```
Algorithm:
function DES_Encrypt (M, K)
where M = (L, R)
    M←IP (M)
    For round←1 to 16 do
        K←SK (K, round)
        L←L xor F(R,Ki)
        swap(L, R)
    end
    swap (L, R)
    M←IP-1(M)
    return M
End
```

B. AES (Advanced Encryption Standard):

The basic steps in algorithm [8] are stated as:

Key Expansion - round keys are derived from the cipher key using Rijndael's key schedule

Initial Round AddRoundKey - each byte of the state is combined with the round key using bitwise xor

RoundsSubBytes - Every byte is replaced with another byte according to a looks towards table by the non-linear substitution

steps.

ShiftRows – The transposition step where each row of the state is shifted cyclically certain number of steps.

MixColumns - A mixing of columns operation which operates on the columns of the state, combining the four bytes in each column is called as MixColumns.

AddRoundKey

Final Round (no MixColumns)- 1. SubBytes 2. ShiftRows 3. AddRoundKey

Key generation- This module handles key generation by the cryptographic module at client side. The server generates

unique keys for users once they authenticate themselves with the server. The key is generated using instances of AES key

generator class. This key is then transferred to the cloud client via the mail-server through a mail which receives and

stores a copy for it for decrypting purpose.

Algorithm

```
Cipher(byte[] input, byte[] output)

{

byte[4,4] State;

copy input[] into State[] AddRoundKey

for (round = 1; round < Nr-1; ++round)

{

SubBytes ShiftRows MixColumns AddRoundKey

}

SubBytes ShiftRows AddRoundKey

copy State[] to output[]

}
```

C. Blowfish Algorithm

This became evolved in 1993. It is one of the most common public algorithms provided by using Bruce Schneier. Blowfish is a variable period key, 64 bit block cipher. No attack is understood to be successful against this. Various experiments and research evaluation proved the prevalence of Blowfish algorithm over different algorithms in terms of the processing time. Blowfish is better than different algorithms in throughput and power consumption [24].

Algorithm:

```
Divide x into two 32-bit halves: xL , xR
For i = 1to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
Next i
Swap xL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xR and xL
```

D. RSA

That is internet encryption and authentication system that makes use of a set of rules developed in 1977 by using Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA set of rules is the maximum commonly used encryption. till now it's far the handiest set of rules used for non-public and public key technology and encryption. it's far a fast encryption [9].

Algorithm

```
Key Generation: KeyGen(p, q)
Input: Two large primes –p, q
Compute n = p. q
φ (n) = (p -1) (q -1)
Choose e such that gcd(e, φ (n)) = 1
Determine d such that e.d ≡ 1 mod φ (n)
Key:
Public key = (e, n)
Secret key= (d, n)
Encryption:
c = me mod n
```

where c is the cipher text and m is the plain text.

RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product. Given ci = E (mi) = mie mod n, then (c1. c2) mod n = (m1 . m2)e mod n

9. CONCLUSION

On this paper, we endorse a singular public key primarily based key-word seek scheme, which supports a multi-owner keyword seek without at ease channels. furthermore, our scheme supports non-interactivity, this means that each facts proprietor and information person within the group can whole his man or woman tasks without interacting with each other. Instead, each of the customers inside the institution handiest wishes to have interaction with the cloud server. furthermore, even though the removal of comfortable channels, our scheme can nonetheless guarantee the comfy key-word seek, with the intention to no longer reveal any extra statistics to the cloud server nor the eavesdropper. In our project work we can deal with security until we not provided secure channels.

ACKNOWLEDGEMENT

“A journey is easier when you travel together. Interdependence is certainly more valuable than independence.”

We take this opportunity to express our deep sense of gratitude and respect to our guide **Mr. Shaikh Sharique Ahmad** without his constant encouragement and key tips it would not have been possible to complete this work with the present quality and we really indebted him for helping us in each aspect of our academic’s activities.

We also owe our sincere thanks to all faculty members of Computer Engineering Department who have been always ready with a helping hand. Last, but not the least, we thank all those people, who have helped us directly or indirectly in accomplishing this work.

I extend a special word to my friends, who have been a constant source of inspiration throughout my project work.

“The completion of any project depends upon the cooperation, coordination, and combined efforts of several resources of knowledge, inspiration, and energy”.

REFERENCES

[1] W.H Sun, W.J Lou, Y.T Hou, and H Li, “Privacy-preserving keyword search over encrypted data in cloud computing,” in Secure Cloud Computing. Springer, 2014, pp. 189–212.

[2] 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.

[3] D Boneh, C.G DI, R Ostrovksy, and G Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.

[4] R Curtmola, J Garay, S Kamara, and R Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[5] J Li, Q Wang, C Wang, N Cao, K Ren, and W.J Lou, "Fuzzy keyword search over encrypted data in cloud computing." in Computer Communications (INFOCOM), IEEE, 2010, pp. 1-5.

[6] C Wang, N Cao, J Li, K Ren, and W.J Lou, "Secure ranked keyword search over encrypted cloud data," in IEEE 30th International Conference on Distributed Computing Systems (ICDCS), 2010, pp. 253–262.

[7] M Li, S.C Yu, N Cao, and W.J Lou, "Authorized private keyword search over encrypted data in cloud computing," in Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011, pp. 383–392.

[8] N Cao, C Wang, M Li, K Ren, and W.J Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[9] W.H Sun, B. Wang, N Cao, M Li, W.J Lou, Y.T Hou, and H Li," Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM, 2013, pp. 71–82.

[10] J Baek, R Safavi-Naini, and W Susilo, "Public key encryption with keyword search revisited," in Computational Science and Its Applications– ICCSA 2008. Springer, 2008, pp. 1249–1259.

[11] H.S Rhee, J.H Park, W Susilo, and D.H Lee, "Improved searchable public key encryption with designated tester," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009, pp. 376–379.

[12] C.X Gu, Y.F Zhu, and H Pan, "Efficient public key encryption with keyword search schemes from pairings," in Information security and cryptology. Springer, 2008, pp. 372–383.

[13] W.H Sun, X.F Liu, W.J Lou, Y.T Hou, and H Li,"Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data," in IEEE Conference on Computer Communications (INFOCOM), 2015, pp. 2110–2118.

[14] B Wang, W Song, W.J Lou, and Y.T Hou, "Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee," in IEEE Conference on Computer Communications (INFOCOM), 2015, pp. 2092–2100.

[15] F Bao, R.H Deng, H.F Zhu, "Variations of diffie- hellman problem," in Information and Communications Security. Springer, 2003, pp.301–312.

[16] "Enron Email Dataset," https://www.cs.cmu.edu/~./enron/.

[17] "Pairing-based Cryptographic Library," https://crypto.stanford.edu/pbc/.

[18] "OpenSSL," https://www.openssl.org/.

[19] B Wang, S Yu, W.J Lou, Y.T Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud." In INFOCOM, 2014 Proceedings, 2014, pp. 2112-2120.

[20] E.J Goh. "Secure Indexes." IACR Cryptology ePrint Archive, pp. 216, 2003.

[21] P Golle, J Staddon, and B Waters. "Secure conjunctive keyword search over encrypted data." In Applied Cryptography and Network Security, 2004, pp. 31-45.

[22] S Kamara, C Papamanthou, and T Roeder," Dynamic searchable symmetric encryption." In Proceedings of the 2012 ACM conference on Computer and communications security, 2012, pp. 965-976.

[23] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[24] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha "Cryptography Algorithm Comparison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[25] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing,"2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC-2010).