ORIGINAL RESEARCH

Secure keyword search using dual encryption in cloud computing

Husna Tariq[1] · Parul Agarwal[1]

Received: 4 July 2017 / Accepted: 18 January 2018 / Published online: 24 January 2018

Abstract This paper manages the secure searching, stockpiling and recovery of client information in the cloud framework. Different services of cloud, security issues and security necessities of cloud information being talked about. We have utilized fuzzy keyword searching scheme to seek and recover the encrypted data by utilizing wild card technique. We have devised a new approach of double encryption framework in light of authentication of the server to give more grounded security to the current fuzzy keyword searching techniques. We have coordinated symmetric and asymmetric encryption algorithms to improve information security. This work, for the most part, concentrates on authentication of the server to enhance the security framework and shield sensitive client's information from unauthorized exposure.

Keywords Dual encryption · Authentication · RSA · AES · Fuzzy keyword search

Abbreviations

AES	Advances encryption algorithm
API	Application Programming Interface
DES	Data encryption standard
DoS	Denial of service
IaaS	Infrastructure as a service
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman algorithm
PaaS	Platform as a service
SSE	Searchable symmetric encryption
SaaS	Software as a service

1 Introduction

The cloud computing provides a web-based platform to varieties of applications running on more than a large number of PCs and servers to simultaneously work together. With the growth of cloud computing now it has turned out to be less demanding for clients to store, recover and share their information among themselves. It offers different advantages to clients and additionally service providers. It gives adaptability to work from anyplace and anytime. It additionally gives low-spending administrations, refreshes programming consequently, raises joint effort among clients and administration sellers and a great deal more [1].

The most broadly embraced utilization of cloud computing is distributed storage. The clients store a huge amount of data on cloud servers consistently. This data needs security from various types of digital dangers [2]. To keep up information privacy and for secure stockpiling, different kinds of encryption techniques are developed for shielding data from unauthorized exposure. Nonetheless, it was difficult to perform searching over encrypted data. But with the introduction of keyword-based searching, this task has become quite easier, and the needed file is retrieved efficiently by providing associated keywords.

The conventional strategies for keyword search were restricted to the exact keyword search. These days, implementation of fuzzy keyword searching has been given by various researchers where the keyword is provided to download the encrypted file even if the keyword is

✉ Parul Agarwal
parul.pragna4@gmail.com

Husna Tariq
husnatariq7@gmail.com

[1] Department of Computer Science, Jamia Hamdard, Hamdard Nagar, New Delhi 110062, India

misspelled and preserving the privacy of keyword in the meantime. Wild card based fuzzy keyword searching has been implemented by Shekokar et al. [3] in a semi-trusted server.

The importance of reliability in performing fuzzy keyword searching has been clearly defined in [4]. According to it, keyword searching is a useful technique so it must be designed efficiently to download the files. Security, availability and performance the required factors to complete it in an efficient manner.

To support data security and information protection, access control and authentication play a crucial role in cloud system [5]. For protecting cloud data, access control techniques are implemented in database management system. When the server is trustworthy, then the working of access control mechanisms is accurate [6]. But access control systems neglects to give the desired security when the server is untrusted [6]. In this manner, the cloud server ought to be reliable and verified with the goal that clients can safely store and recover their information.

So the objective of this paper is to center towards the execution of authentication next to the server. Clients must have the capacity to confirm whether his downloaded information originates from a trusted source or not. So to give extra security and protection to the fuzzy keyword searching strategy in the cloud framework, we have recommended a thought of double encryption that joins the upside of symmetric and asymmetric encryption algorithm. The proposed implementation work adds RSA algorithm to encrypt the message using server's private key before the file is downloaded at client's end. This is done so that client can verify the authenticity of server and confirm whether the message originates from a claimed source or not. We named our encryption algorithm as dual encryption algorithm.

2 Cloud services, its issues and requirements

In the cloud network, a security breach could occur at any of the component. The cloud contains three entities as indicated by [7]:

- User: The person who is keen on using the administrations of cloud specialist organizations. It can be singular client, firm or any association. They rely on upon the cloud to store their important data and information.
- Cloud service provider: This entity has the specialist to deal with the servers scattered at various areas, and it controls entire distributed computing framework since it gives critical assets and skill to clients.
- Third party auditor: It is utilized as a part of the circumstance where the client does not have obliged assets to profit the administrations of the cloud. Hence it is an optional case.

2.1 Cloud services

The cloud services are based upon three advanced models which are platform as a service, software as a service and infrastructure as a service. Depending upon the request and necessity of their applications, these services are given to clients [3, 8]. Cloud service providers outline three particular layers to actualize distinctive innovations in cloud framework which are:

2.1.1 Infrastructure as a service

This level is responsible for doing the assignment of administration and capacity of cloud assets. Regularly cloud works on virtual assets, and along these lines, clients can have admittance to an assortment of virtual assets like servers, equipment, programming, and so on that are given to clients to satisfy application's necessity [9].

2.1.2 Platform as a service

The following level gives the platform to create programming and applications. It encourages administration and deployment of client's application. The service providers provide hardware and software tools to develop applications [10]. It additionally obliges application systems to bolster software as a service.

2.1.3 Software as a service

This level gives the most predominant administration which empowers the cloud clients to collaborate with the application. There is no compelling reason to introduce equipment and programming assets at client's place [11]. It is user's application where there is no need to concentrate on infrastructure management and service upkeeping.

2.2 Cloud security issues

In spite of these preferences, we have a lot of security issues identified with cloud benefits because of which numerous associations and clients are unwilling to take cloud benefits. A portion of the security issues is depicted by [12].

2.2.1 Data breaches

It happens when the highly confidential and classified data of clients put away in the cloud is stolen, seen and consequently presented to unauthorized elements [13]. It incorporates trade secrets, bank account details and so on.

2.2.2 Account hijacking

It is the procedure where the hacker hijacks the login details of the client and utilize it for doing some unapproved or noxious actions on remotely put away cloud information of the client [14].

2.2.3 Insider attacks (threat)

In this approved worker of an association abuses his conceded benefits to access client's confidential data like account details, budgetary structures, and so on. The majority of the organizations don't concentrate much towards this attack because their essential concentration is towards outside assaults [15].

2.2.4 Malware infusion

It occurs when the cloud administrations are installed with code or scripts that perform like "legitimate instance" and work as SaaS on cloud server [16]. It seems to do the coherent operation, regardless, it helps hackers to monitor and listen in and take the confidential data.

2.2.5 Denial of service attack

It attacks availability service of the cloud network. The attacker tries to flood the cloud framework, system, and administrations so that authorized clients are not ready to utilize them [17].

2.2.6 Data loss

Data loss can happen through a vindictive assault and catastrophic event like natural disasters. It can likewise occur because of the absence of recuperation plan and mismanagement and improper administration of cloud information [18].

2.2.7 Insecure APIs

Application Programming Interfaces are utilized to modify the features of administrations given by cloud as per the business requirements [19]. With the development of its framework, security hazard additionally increments. Uncertainty in the API lies in the correspondence which happens between applications.

2.3 Cloud security requirements

In spite of the fact that the administrations given by the cloud are frequently being enhanced, still, there is an extraordinary requirement for security and protection of information stored in the cloud. For this, an essential prerequisite is to develop trust between the client and service vendors. The cloud framework must be sufficiently proficient in executing the fitting safety efforts at its premises.

To ensure cloud information, taking after safety efforts should be actualized [20]:

2.3.1 Authentication

This system assists the entities involved in communication with proving its identity and guarantees genuine correspondence [21]. This administration additionally ensures that no other unapproved element can disguise itself as approved element to take undue benefits of progressing correspondence.

2.3.2 Access control

It is the way of forcing the restriction to get access to frameworks and applications as per the level of security necessities [21]. Verification and authentication must be done to give rights to the entity.

2.3.3 Confidentiality

The information must be protected from unauthorized exposure so that confidentiality is maintained. Unauthorized presentation of data must be ensured to keep up the privacy of touchy cloud information [21]. The attacker is not permitted to take a gander at recurrence, length and different traits of activity moving through the system.

2.3.4 Integrity

This administration guarantees the rightness and legitimacy of information being transmitted through the system. The got information must be free from duplication, adjustment, and reordering [21]. Only approved clients can roll out improvements to it.

2.3.5 Availability

It guarantees that data is accessible to only authorized clients at whatever point required [21]. To keep up it offsite backup ought to be done routinely, and the frameworks must be avoided by Denial of service assaults.

2.3.6 Non-repudiation

This administration assures the confirmation that the alleged sender and receiver has sent and got the data respectively [21]. To implement it, precise, traceable records must be kept up.

3 Literature survey

Song et al. [22] had proposed an idea where separate encryption on each word of the document was done. As it required the word to word examining the documents, this system brought about higher cost. So this plan was not effective. They proposed a sequential scan that could be performed with or without an index. At the point when the records in the dataset are massive, then the indexed based plan is favored because it gives speedier indexed lists and thus provides faster results. In any case, this framework causes inconvenience in the circumstance where capacity and refreshing of records are required.

To make the looking procedure more easy to understand, Wang et al. [23] recommended a secure ranked keyword search strategy in which the coordinating documents are returned in a positioned arrange contingent upon certain pertinent standards like frequency of keywords, and so forth. Wang et al. [23] prompted a searchable symmetric encryption (SSE) and showed its inefficiency. Later they outlined an order-preserving symmetric encryption scheme to convey enhanced security rather than SSE framework, together with the upside of ranking outcomes.

Wang et al. [24] later carried on to advance the idea of an encrypted invert index to achieve secure ranked search in encrypted cloud data. It was gone for computing the significance score amongst query and records. Depending on the significance scored computed, records are ranked with the goal that clients can get most significant n outcome. It was seen that because of the absence of ranking strategy, lots of client time is squandered on hunting down required data from a tremendous measure of records. So Li et al. [25] presented and connected the idea of order preserving methods for quicker retrieval of documents.

Boneh et al. [26] proposed the possibility of public key encryption framework where keyword seeking technique is done on encrypted information. This approach utilizes the public key to store data in the cloud and uses private key for performing the searching process. Ballard et al. [27] framed conjunctive keyword searching strategies to improve the searching system. In any case, these strategies brought about critical overhead costs in correspondence because of sharing the secret and expanded computational expenses because of bilinear mapping.

Privacy-preserving, similarity based text retrieval scheme was given by Pang et al. [28] where the search outcomes are concealed from the unauthorized entities of the network. Additionally, the server can't reproduce the term composition of records and performing queries. They utilized likeness measure of "coordinated matching" sorted out as multi-keyword semantics. To quantitatively assess the likeness measure it utilizes "inner product similarity". But there were two inadequacies of this plan. Above all else, it requires the rearrangement of static dictionary every time with the addition of new keyword. But when the size of the accumulation of records becomes exponentially large, then the time required for searching process likewise increments exponentially.

Cao et al. [29] proposed a superior scheme in which calculations was lessened with the expansion in the size of keyword dictionary. In this scheme, keyword's access frequencies were also taken into account. Be this plan was not easy to use as it doesn't have the elements of semantics and fuzzy keywords.

Fuzzy keyword searching was introduced over encrypted cloud data for the more user-friendly searching procedure. At first, the idea of fuzzy keyword searching for encrypted cloud data was given by Li et al. [30]. This strategy endeavored to make the search technique user interactive. It expresses that the search system utilized as a part of this technique can give the exact outcome regardless of the possibility that the keyword is somewhat incorrectly spelled by the user. Then again, in conventional systems, no outcome is found when there are minor mistakes in spelling of inputted keyword, and subsequently, it makes the user's undertaking extremely confused. To deal with this issue, Li et al. [30] executed fuzzy keyword searching. That, as well as focus on safeguarding the security of keywords. If user spell mistakenly then edit distance technique is utilized by fuzzy keyword to compute the closest matching keyword. To reduce the trouble away and to deal with the issues in portrayal, they created keyword dictionary. They showed that their work was capable of keeping up the protection and security in place. It additionally demonstrated the utility of fuzzy keyword searching procedure.

Khan et al. [31] attempted to improve the past works in this field by including the ranking usefulness together with multi-keyword searching over encrypted cloud information and hence improved the search procedure. This method considered the importance of results by some matched keywords. Be that as it may, this method did not rank the outcomes internally, and furthermore, the synonym searching was not contemplated. Subsequently, the searching time was highly expanded.

To verify the efficiency, integrity, and accuracy of results, Chai and Gong [32] displayed a verifiable search procedure. Wang et al. [33] upheld a fuzzy keyword searching technique which considered verification in view of VSSE (verifiable symmetric searchable encryption). However, this plan fails to rank outcomes. Additionally, synonym based multi keyword search framework was recommended by Fu et al. [34] in an encrypted cloud. It may be conceivable that user forgets the correct keyword. At that point, the client can do searching by similar meaning words.

4 Algorithms and techniques used

4.1 Fuzzy keyword searching using wildcard

Fuzzy keyword searching is a searching method in which matching is performed in such a way the right outcome is returned regardless of the possibility that the entered word is deficient or marginally incorrectly spelled. Fuzzy searching is performed on keywords which give the usefulness of downloading documents.

The wild card is a character which can represent more than one other character, and it is utilized to maximize search results [35]. For term or query, Wildcard technique is an interactive searching strategy. The wild card is used to signify edit distance. The edit distance ed (w1, w2) is the number of operations needed to transform one word to another word among two words w1 and w2 [36]. The edit distance has three operations.

1. Substitution: In a word, transform one character to another character.
2. Erasure: Deletes one character from a word.
3. Addition: Adds one character to a word.

In this technique, if the operation is performed in the same position then all choices is checked. For instance, if the pre-edit distance is set to 1 for the word CASTLE then S_{CASTLE}, 1 = {CASTLE, *CASTLE, *ASTLE, C*ASTLE, C*STLE, CASTL*E, CASTL*, CASTLE*}. Here aggregate number of variations is 13 + 1, instead of 13 × 26 + 1.

4.2 Algorithms used for encryption and decryption process

We have utilized two sorts of encryption algorithm to do the way toward transferring and downloading of documents. AES has been utilized as symmetric encryption, and RSA has been utilized as asymmetric encryption.

4.2.1 Advanced encryption standard (AES) algorithm

We are considering about AES for encryption reason since it is viewed as most secure encryption calculation till now [37, 38]. It is likewise quicker hardware and software implementation when contrasted with DES and RSA [39]. AES is symmetric encryption algorithm since the same key is utilized for encryption and also for decryption. In this algorithm input data is processed as blocks of size 128 bits. It has three particular key sizes: 128, 192 and 256 bits which rely on upon the number of rounds. In a large portion of the cases, the key size of 128 bits is picked [21]. So we have picked the key size of 128 bits which has ten processing rounds for encryption.

4.2.2 RSA algorithm

Ron Rivest, Adi Shamir, and Leonard Adleman built up an asymmetric encryption algorithm which utilized two diverse keys for encryption and decryption. One is named as public key and alternate as the private key [21]. As the name demonstrate, the public key is known to every user of the system and the private key is kept secret. For authentication, the message is encrypted with the private key, and for secrecy, the message is encrypted with the public key. For decryption of created ciphertext, inverse keys are utilized. Both the keys are mathematically connected to each other [21].

Out of the two keys, one is utilized to scramble, and the other is utilized to unscramble the message. RSA is considered as most widely utilized asymmetric encryption algorithm as it offers confidentiality, integrity, authentication and non-repudiation services to data storage and communication [40].

RSA is secure because multiplication of prime number utilized is simple. However, estimation of the original prime number from the aggregate is difficult to figure as it would require a lot of time [40].

5 Problem formulation

We manage cloud client, cloud server in the cloud. We have n encrypted files F = (F1, F2, F3, …, Fn) and keywords K = (K1, K2, K3,…, Kn) stored in cloud server. At that point approved clients are permitted to look and search their coveted documents over the encrypted information F in the cloud using keyword K.

Legitimate approval is considered between the client and server in the cloud. The client inputs his demand to cloud framework to get his needed files. Documents are put away on the server in view of record Id and each of them the is mapped to keywords connected with them. The cloud server relates every request of keyword search for with the applicable records. The accompanying standards are taken after for recovering the required records the following rules are followed in view of fuzzy keyword searching:

1. In the event that the inputted keyword exactly matches with the stored keyword, at that point the server must return document comparing to given keyword.
2. On the off chance that there exist any spelling mistake or dissimilarity with the saved keyword, at that point the server must restore the closest likely outcome by pre-determined similarity semantics.

At the point when the keyword based searching is done in the cloud, at that point it may be conceivable that any unapproved element endeavors to imitate as the true server and attempt to access some confidential data inspite of secure AES encryption. Therefore, the searching system ought to be performed such that the client can verify the server before recovering records. To accomplish this, we have incorporated RSA encryption algorithm alongside AES algorithm for secure record recovery from the cloud server.

This paper offers a proficient answer for cloud clients to confirm the realness of server and safely store and recover their required information to and from the cloud. The point of this paper is to

1. To give strong authentication to the server with the goal that clients can download documents safely.
2. To devise a search system in view of the created fuzzy keyword searching strategy.
3. To give the security to above-outlined data recovery framework by adding RSA algorithm to AES algorithm.

6 Proposed work

Approved clients are included by the organisation who require access to their information. The client enters the query for retrieving his document by inputting the keyword. The entered keyword is matched with the saved keyword. On the off chance that it matches, at that point the desired record is sent back to the client after decrypting. We have developed a strong server authentication framework over the saved encrypted information. Procedures executed up to now has focussed on fuzzy keyword searching on encrypted cloud information. In this work, we have included double encryption by implementing the blend of the symmetric and asymmetric algorithm.

7 Proposed algorithm

7.1 When user uploads file

1. It involves a single symmetric encryption algorithm AES.
2. The user file F is encrypted with secret key Ks to produce encrypted file F' which is stored at the server as shown in Fig. 1.

7.2 When user downloads file

1. It involves the combination of symmetric encryption algorithm AES and asymmetric encryption algorithm RSA.
2. The encrypted file F' stored at server is encrypted again using RSA to produce doubly encrypted file F'' with server's private key and sent to user.
3. The user decrypts doubly encrypted file F'' using RSA to generate an encrypted file F' with server's public key.
4. Finally, the user decrypts the received encrypted file F' to produce the original file F with his secret key as shown in Fig. 2.

7.3 Notations

K:	Keyword
K':	Encrypted keyword
K_{search}:	Search keyword
F:	User file
F':	Encrypted file
F'':	Double encrypted file
K_S:	Secret key of user
K_{PR}:	Private key of server
K_{PU}:	Public key of server
E_{AES}:	Encryption using AES algorithm
E_{RSA}:	Encryption using RSA algorithm
D_{AES}:	Decryption using AES algorithm
D_{RSA}:	Decryption using RSA algorithm

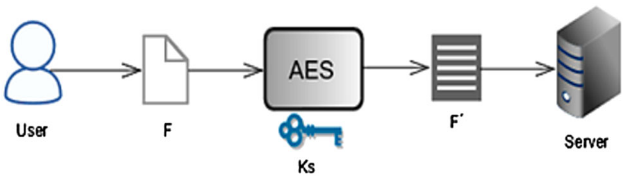


Fig. 1 File upload process

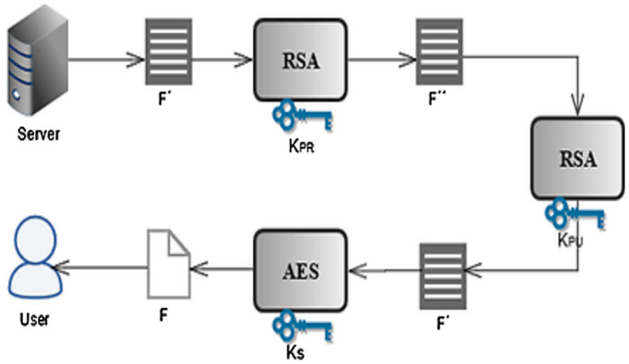


Fig. 2 File download process

7.3.1 User uploads the corresponding file in encrypted form

$$E_{AES}(K_S, K) \rightarrow K'$$

$$E_{AES}(K_S, F) \rightarrow F'$$

7.3.2 User perform search and downloads his file

```
STEP 1. $K_{SEARCH} \leftarrow$ User Input
             $E_{AES}(K_S, K) \rightarrow K'$

               IF MATCHES FOUND
               THEN GO TO STEP 2
               ELSE
             NO RESULT FOUND

STEP 2. DOWNLOAD FILE

             Encryption by server
$E_{RSA}(K_{PR}, F') \rightarrow F''$

             Decryption by user
             $D_{RSA}(K_{PU}, F'') \rightarrow F'$
             $D_{AES}(K_S, F') \rightarrow F$
```

7.4 Steps for proposed algorithm

The proposed dual encryption performed as follows:

- The user authenticates himself by providing user Id and password to the cloud server.
- After the authentication process, the server request user to enter the keyword and upload his file.
- The keyword entered is stored in encrypted form using AES at the server.
- The user uploads the file F that is encrypted with AES algorithm and generated cipher F' is stored on the server. The encryption is done using secret key Ks.
- The process of dual encryption comes into the picture whenever the user needs to download his desired file. The server asks the user to enter the keyword to download the corresponding file.
- The keyword entered by the user is matched to the stored keywords. If it matches according to rules, then the corresponding file is encrypted using RSA.
- To prove its authenticity, the server uses RSA algorithm to encrypt the encrypted file F' with its private key and send the generated encrypted file F'' to the user. Here the dual encryption on F' using server's private key is done to provide authentication of cloud server.
- The user receives F'' and decrypts it with the server's public key to get the F' using RSA.
- The F' is again decrypted with the secret key Ks using AES to give the original file F to the user.
- Hence the user retrieves his desired file in a secure manner along with the verification of authenticity of the source as shown in Fig. 3.

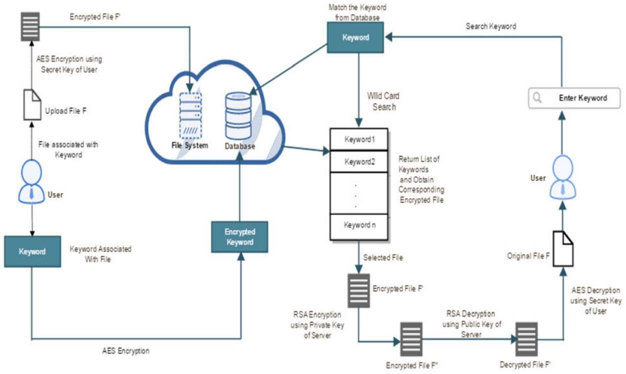

Encrypted File F'
AES Encryption using Secret Key of User
Upload File F
File associated with Keyword
User
Keyword
Keyword Associated With File
AES Encryption
File System
Database
Encrypted Keyword
Match the Keyword from Database
Keyword
Search Keyword
Wild Card Search
Keyword1
Keyword2
Keyword n
Return List of Keywords and Obtain Corresponding Encrypted File
Enter Keyword
User
Original File F
Selected File
Encrypted File F'
RSA Encryption using Private Key of Server
Encrypted File F''
RSA Decryption using Public Key of Server
Decrypted File F'
AES Decryption using Secret Key of User

Fig. 3 System architecture for fuzzy keyword search using dual encryption algorithm

8 System architecture for searching using dual encryption

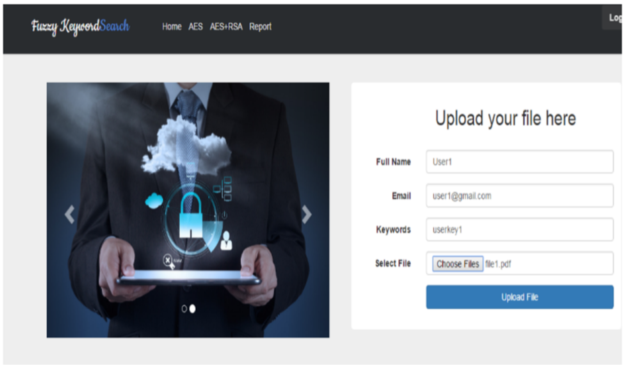
8.1 Implementation

We have used JDK environment to execute the algorithms. We are figuring the aggregate time required to transfer and after that download the document. Subsequently we are consolidating the encryption and decryption time for the entire cycle.

According to our proposed scheme, we are applying the process of dual encryption and decryption only when the user intends to download the file. Keyword inputted by the user is stored at cloud server in encrypted form by using AES algorithm. Encrypted keyword and encrypted files are stored on server using AES as shown in Fig. 5. When user demands a particular file then he enters the keyword to get the corresponding file. This is performed by matching the keyword and the file stored which was uploaded along with that particular keyword. So, basically we are doing the dual transformation on the file only, and not on the keyword stored.

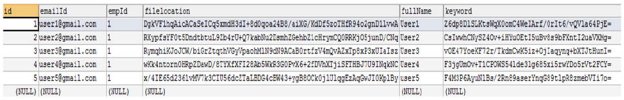
Before the file and the keyword get stored on the server, the server will confirm to verify the correctness of keyword so as to make sure that the user has entered a correct keyword and file. But at the time of downloading the required file, it might happen that the user forgets his keyword. Although he posses the shared secret key, he cannot download his desired file because he is unable to give the correct keyword so that matching with the needed file could be done.

The proposed scheme also takes the email id of user along with the file and keyword which is shown in Fig. 4. When a user enters his details regarding his name, email id, file to be uploaded and keyword associated with that file, then at the same time the cloud server sends an acknowledgement on that email id stating the details of information entered.



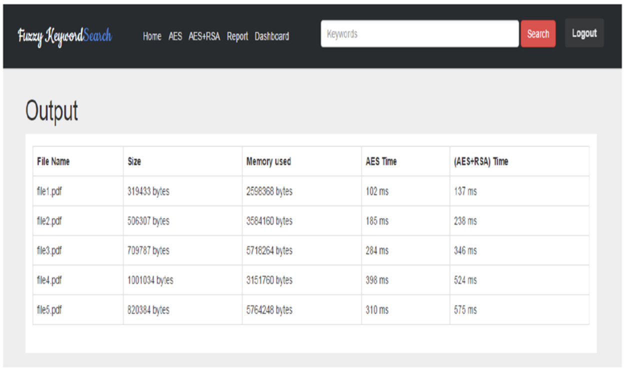
Full Name: User1
Email: user1@gmail.com
Keywords: userkey1
Select File: file1.pdf

Fig. 4 Screenshot-file upload



id	emailId	empId	filelocation	fullName	keyword
1	user1@gmail.com	1	DgkVF1hqAicACaSeICq5xmdH3dI+8d0qoa24B8/aiXG/KdDf5zoTHfR94o2gnD1LvwA	User1	Z6dp8D1SLKtsWqX0omC4WeIArf/0rIt6/vQVla64PjE=
2	user2@gmail.com	1	RXypfsYF0t5DndtbtuL9Zb4rU+Q7kabNu2DsmhZGehbZicHrymCQ0RRKjO5junD/CNq	User2	CsIwwhCNySZ40v+iHYuOEtI5uBv8s9bFXntI2uaVXMg=
3	user3@gmail.com	1	RymqhiKJoJCW/biGrZtqthVGyVpaohMlN9dN9ACaB0rtfzV4mQvAZxTp8xP3xUIaIsz	User3	vOE47YoeKF72r/TkdmCwK5iz+OjIaqynq+bXTJtHunI=
4	user4@gmail.com	1	wKk4ntorn0HRpZDawD/8TYXfXFI28Ab5WkR3G0PvX6+2fDVhXTjiSFTHBJ7U9INqkNC	User4	F3jgUmOv+T1CPOWS54lde3lg685xi5rwYDo5rVt2FCY=
5	user5@gmail.com	1	x/4IE65d2361vMV7k3CIU56dcZTaLBDG4cBW43+ygB8OCk0j1UlqgEzAqGwJI0KplBy	user5	F4M3P6AyuN1Bs/2Rn69aserYnqG89tlpR8zmebVIi7o=
(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)

Fig. 5 Keyword stored in encrypted form at server



Output

File Name	Size	Memory used	AES Time	(AES+RSA) Time
file1.pdf	319433 bytes	2598368 bytes	102 ms	137 ms
file2.pdf	506307 bytes	3584160 bytes	185 ms	238 ms
file3.pdf	709787 bytes	5718264 bytes	284 ms	346 ms
file4.pdf	1001034 bytes	3151760 bytes	398 ms	524 ms
file5.pdf	820384 bytes	5764248 bytes	310 ms	575 ms

Fig. 6 Generated output

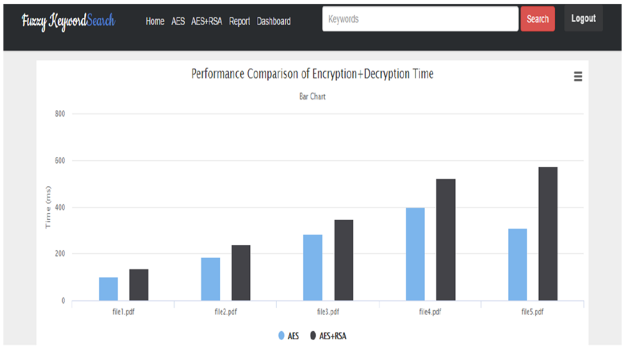


Fig. 7 Performance comparison of encryption + decryption time for 5 files

Therefore, whenever the user forgets or unknowingly save a keyword then he can request the server to send a new keyword to download his file. The server makes and sends a new random keyword to the user. The user enters the new keyword which is then matched to give out the associated file so that the user could download his needed file. Since the user has the secret key, he can easily decrypt it.

For extra security, the server can ask for time and date of entering the records of user. After taking the details of it, the server can match it with the stored records and verify whether the request has come from an authentic user or not.

1. User is requested to enter keyword and upload the associated file as shown in Fig. 4.
2. The server stores the keyword in encrypted form in database as shown in Fig. 5.

3. User download the files using existing (AES) encryption algorithm and the proposed (AES+RSA) dual encryption algorithm, and the output generated is represented in Fig. 6.
4. Bar chart representation of both algorithm is shown in Fig. 7. Which shows the total time required to complete the cycle. One cycle is equal to time required for encryption to store the file on server plus the time required for decryption to retrieve the file from the server. We are comparing the results using five files. Time is measured in milliseconds.

9 Results

By utilizing AES encryption, fuzzy keyword search is performed. However, the proposed keyword searching scheme actualizes it utilizing the mix of AES and RSA calculation which is named as the double encryption algorithm. The comparison of performance between the both algorithms is demonstrated in Fig. 7. It is concluded that the proposed algorithm takes more time as compared to existing algorithm.

Our proposed plan is joining RSA and AES so authentication is additionally furnished alongside security. In spite of the fact that our plan is slower than conventional methods, it can perform better in circumstances where authentication is needed.

To perform fuzzy keyword search, the client store his document alongside the associated keyword so as to perform fuzzy keyword search and later downloads the record by utilizing the same keyword in a safe manner. The client can check that his document is downloaded from a valid server.

10 Conclusion

This paper proposes a productive and secure keyword based searching plan where the client can store his documents in a safe way. To make the searching strategy user friendly, fuzzy keyword searching is presented utilizing the wild card system. We have semi-trusted cloud server where the client's information is put away in scrambled form to keep server and unauthentic entity from adapting any data in regards to the stored client's information. To give solid security, the proposed double encryption calculation checks the genuineness of the cloud server on the grounds that the document is encrypted with server's private key before it is sent to the client. When we discuss security, without a doubt asymmetric algorithm ends up being the most secure algorithm. Hence, the blend of symmetric, and additionally the asymmetric algorithm, makes the encryption procedure more confused to crack by unapproved elements of the cloud network. Along these lines, the cloud framework turns out to be more impervious to various security assaults performed by unapproved entities who attempt to unveil the delicate client's data for their advantages.

References

1. Avram MG (2014) Advantages and challenges of adopting cloud computing from an enterprise perspective. In: Proceedings of the 7th international conference interdisciplinarity in engineering, INTER-ENG 2013, vol 12. pp 529–534
2. Vurukona N, Rao BT (2016) A study on data storage security issues in cloud computing. In: Proceedings of 2nd international conference on intelligent computing, communication and convergence, ICCC-2016 held in Bhubaneswar, Odisha, India, vol 92. pp 128–135
3. Shekokar N, Sampat K, Chandawalla C, Shah J (2015) Implementation of fuzzy keyword search over encrypted data in cloud computing. In: Proceedings of international conference on advanced computing technologies and applications (ICACTA-2015) held in Mumbai, India, ISBN: 978-1-5108-0136-3, vol 45. pp 499–505
4. Hegde D, Saritha (2014) Secure fuzzy keyword search using an advanced technique over an encrypted cloud data. Int J Eng Comput Sci 3(3): 5102–5104
5. Mahajan N, Patil D (2016) Study of authentication and authorization in cloud computing. Int J Recent Innov Trends Comput Commun 4(7):178–180
6. Zhao Y, Chen X, Ma H, Tang Q, Zhu H (2012) A new trapdoor-indistinguishable public key encryption with keyword search. J Wirel Mob Netw Ubiquitous Comput Dependable Appl (JoWUA) 3(½):72–81
7. Kokane M, Jain P, Sarandhar P (2013) Data storage security in cloud computing. Int J Adv Res Comput Commun Eng 2(3):1388–1393
8. Singh R, Kumar S, Agrahari SK (2012) Ensuring data storage security in cloud computing. IOSR J Eng 2(12):17–21
9. Bhardwaj S, Jain L, Jain S (2010) Cloud computing: a study of infrastructure as a service (IAAS). Int J Eng Inf Technol 2(1):60–63
10. Kulkarni G, Khatawkar P, Gambhir J (2011) Cloud computing—platform as a service. Int J Eng Adv Technol (IJEAT) 1(2):115–120
11. Rashmi G Sahoo, Mehfuz S (2013) Securing software as a service model of cloud computing: issues and solutions. Int J Cloud Comput Serv Archit (IJCCSA) 3(4):1–11
12. Ahmed M, Hossain MA (2014) Cloud computing and security issues in the cloud. Int J Netw Sec Appl (IJNSA) 6(1):25–36
13. Barona R, Anita EAM (2017) A survey on data breach challenges in cloud computing security: issues and threats. In: International conference on circuit, power and computing technologies (ICCPCT-2017) held in Kollam, India, ISBN: 978-1-5090-4967-7. pp 20–21
14. Christina AA (2015) Proactive measures on account hijacking in cloud computing network. Asian J Comput Sci Technol 4(2):31–34
15. Yusop ZM, Abawajy JH (2013) Analysis of insiders attack mitigation strategies. In: International conference on innovation,

management and technology research held in Malaysia, vol 129. pp 611–618

16. Watson MR, Shirazi NH, Marnerides AK, Mauthe A, Hutchison D (2016) Malware detection in cloud computing infrastructures. IEEE Trans Dependable Secure Comput 13(2):192–205
17. Carlin A, Hammoudeh M, Aldabbas O (2015) Defense for distributed denial of service attacks in cloud computing. In: International conference on advanced wireless, information, and communication technologies (AWICT-2015), vol 73. pp 490–497
18. Wong R (2017) Research on data security technology based on cloud storage. In: 13th global congress on manufacturing and management, (GCMM-2016). pp 1340–1355
19. Wickramasinghe SKH, Sudesh RMC, Dissanayaka DKGM, Udarini WAN, Hettiarachchi PHAI, Dhammearatchi D (2016) Cloud computing-enhancement of security with respect to encryption and secure APIs. Imp J Interdiscip Res (IJIR) 2(5):690–695
20. Revalla M, Gupta A, Bhuse V (2013) On providing user-level data privacy in cloud. In: Proceedings of the international conference on cloud security management, ISBN: 978-1-909507-69-2. pp 106–114
21. Stallings W (2011) Cryptography and network security: principle and practice, 5th edn. Pearson, London
22. Song DX, Wagner D, Perrig A (2000) Practical techniques for searches on encrypted data. In: Proceedings of IEEE symposium on security and privacy, ISBN:0-7695-0665-8. pp 44–55
23. Wang C, Cao N, Li J, Ren K, Lou WJ (2010) Secure ranked keyword search over encrypted cloud data. In: Proceedings of IEEE 30th international conference on distributed computing systems (ICDCS). pp 253–262
24. Wang C, Cao N, Ren K, Lou WJ (2012) Enabling secure and efficient ranked keyword search over outsourced cloud data. IEEE Trans Parallel Distrib Syst 23(8):1467–1479
25. Li K, Zhang W, Yang C, Yu N (2015) Security analysis on one to-many order preserving encryption-based cloud data search. IEEE Trans Inf Forensics Secur 10(9):1918–1926
26. Boneh D, Crescenzo GD, Ostrovsky R, Persiano G (2004) Public key encryption with keyword search. In: Proceedings of eurocrypt, LNCS 3027. pp 506–522
27. Ballard L, Kamara S, Monrose F (2005) Achieving efficient conjunctive keyword searches over encrypted data. In: Proceedings of 7th international conference on information and communications security, ICICS 2005 held in Beijing, China, vol 3783 LNCS, ISSN 03029743. pp 414–426
28. Pang H, Shen J, Krishnan R (2010) Privacy-preserving similarity-based text retrieval. ACM Trans Internet Technol (TOIT) 10(1):39–42
29. Cao N, Wang C, Li M, Ren K, Lou WJ (2011) Privacy-preserving multi-keyword ranked search over encrypted cloud data. In: Proceedings of IEEE INFOCOM, 2011. pp 829–837
30. Li J, Wang Q, Wang C, Cao N, Ren K, Lou WJ (2010) Fuzzy keyword search over encrypted data in cloud computing. In: Proceedings of IEEE INFOCOM. pp 1–5
31. Khan N, Krishna CR, Khurana A (2014) Secure fuzzy multi-keyword search over outsourced encrypted cloud data. In: Proceedings of IEEE international conference on computer and communication technology (ICCCT). pp 241–249
32. Chai Q, Gong G (2012) Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers. In: Proceedings of IEEE international conference on communications (ICC'12). pp 917–922
33. Wang J, Ma H, Tang Q, Li J, Zhu H, Ma S, Chen X (2012) A new efficient verifiable fuzzy keyword search scheme. J Wirel Mob Netw Ubiquitous Comput Dependable Appl 3(4):61–71
34. Fu Z, Sun X, Linge N, Zhou L (2014) Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query. IEEE Trans Consum Electron 60(1):164–172
35. Satapathy SK, Mishra S, Mishra D (2010) Search technique using wildcards or truncation: a tolerance rough set clustering approach. Int J Adv Comput Sci Appl (IJACSA) 1(4):73–77
36. Mishra S, Satapathy SK, Mishra D (2009) Improved search technique using wildcards or truncation. In: Proceedings of international conference on intelligent agent & multi-agent systems, IAMA 2009. pp. 1–4
37. Kashyap S, Madan N (2015) A review on: network security and cryptographic algorithm. Int J Adv Res Comput Sci Softw Eng 5(4):1414–1418
38. P. Krithika, G. Dilipan and M. Shobana (2015) Enhancing cloud computing security for data sharing within group members. IOSR J Comput Eng (IOSR-JCE) 17(2):110–114
39. Mahajan P, Sachdeva A (2013) A study of encryption algorithms AES, DES, and RSA for security. Glob J Comput Sci Technol Netw Web Sec 13(15):15–22
40. Preetha M, Nithya M (2013) A study and performance analysis of RSA algorithm. Int J Comput Sci Mob Comput (IJCSMC) 2(6):126–139