JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 26 Issue 01, 2023 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

A SECRECY-CONSERVING MULTI-USER ACCESS AND MULTI-KEYWORD SEARCH AES FOR DISTRIBUTION SYSTEM

S. Surya Teja [1], Dr. K. F. Bharati [2]

[1]M.Tech Student, Department of CSE (AI), JNTUA, Anantapuram, Andhra Pradesh, India

[2]Associate professor, Department of CSE, JNTUA, Anantapuram, Andhra Pradesh, India

surusuryateja1998@gmail.com1, kfbharati.cse@jntua.ac.in2

Abstract

To protect the data search and retrieval process, the cloud stores large files in various forms such as Google Drive, iDrive, and Dropbox in a distributed environment. A searchable encryption technique is used to achieve the desired functionality and security/privacy. It states that the most difficult task will be eliminated by providing multi-keyword search, multi-user settings, and access patterns to eliminate the Key Generation Center (KGA). In this study, I specifically introduced novel encryption schemes such as the AES and ELGAMAL schemes. The application is user-friendly. Finally, I am able to demonstrate the process's secure computation and communication between the CP and IS.

Keywords: Security, AES, KGA, Multi-User, ELGAMAL, CP, IS

Introduction

When compared to traditional data storage methods, cloud storage has grown in popularity among both personal and individual users. The cloud computing process will include five columns. Before the page appears and we are required to log in because the access is provided by cloud services, we must first visit the data provider and complete a new registration in which we enter our information, and then we must go to the CP [17]. The paper discusses clouds, cloud storage, and service providers on the basis of different parameters such as pricing, maximum storage limit, and security of data after that, Then we will open the data provider and it will show the view details of the data provider, that is, the serial number means numbers will be present, the DP name means person names will be present, the email id means user email id will be present, the address will be present, what user has uploaded the details it will present, and registration date means when the user registered it will show them, and the status means whether it is in the request or accept state will be Cloud must accept or reject the details, then accept the details, and navigate to the data provider. In the data provider, after work is done, it will show the successful page next to the person's name. The homepage, view files, and upload files columns all are present in the data provider. Upload files indicate that the file name, parameters, algorithms, servers, upload files, and upload option all will be present on the file upload page. Here "file name" means files; it has some names like "files," "my files," server means there are three servers in the cloud: server 1, server 2, and server 3; and upload files means there is a choose file option; then we will choose the files we want to upload and click the upload them. It shows the file that was uploaded, then we go to view files and see the file name, server type, and encryption form to see what that means.

AES algorithms [15], this algorithm has its own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world, indicating that they

Submitted: 17/12/2022 **Accepted**: 10/01/2023

will display no format (binary form). Whereas ELGAMAL [16] is a public key encryption algorithm that is put practice into for information transmission. It indicates that it will display the numbers repeatedly done on the data provider. Come to the homepage, and then go to the user page where we want to register users, and it will show the registration page of the process. Fill in the details of the users, then submit. But it will not, because the cloud wants to accept the details. After there is a user request column; click on it to see the user's details; click Accept to accept the details. Go to the user page, in as that user on the home page, search for files, and download files. Search file means that we want to search what we upload in DP files; it will show file owner name, file name, server name, view file data, and status (request form is present), then send request, it will show request send to the cloud. Go to the cloud login, there is a column for user requests files, click it in that data owner email id, user email id, file name, server name, file id, and accept. It will indicate that the request was accepted, and that data was shared with the internal server. Then navigate to the internal server page, where an internal server login page will be displayed.

On the internal server, it has a homepage, views the server details, requests files, and allows you to. Then go to the requested files, which have an email id, User email id, File name, File id, Server name, and Action. It has taken action by generating a key, which is now present in columns. Then the process of generating the key; will load a page after that OTP came to the user's email; copy it will show the key sent to the user; there is a "download file" column. File name, File id, Status, and Download are all included in that file. It has opened the file in that download. In the download file, it has entered the key values that we get in the mail, like "OTP". It will save the downloaded file in some download files. The file is open in Notepad, and we see the file of the process; thus, we will upload multiple files, and we can download multiple times of the process.

Contribution

In this study, we provide a new public-key searchable encryption, which necessitates the usage of a hybrid model in the scheme to solve security, privacy, and functionality concerns. The method can be applied on many specified servers to let the public key cloud storage server carry out a multi-keyword search over encrypted data while protecting privacy in dispersed contexts with various data writers and users. Our approach, Searchable Encryption is based on a productive, externally calculated structure with various keys that protect privacy.

To determine whether one input set is a subset of the other input set, I create new subset determination procedures. The suggested procedures served as the foundation for the multi-keyword search functionality in a two-server design. It will be helpful for other procedures that call for testing on private subsets.

The basic main method of our scheme's subset decision processes. The benefits of the suggested plan include support for multiple users, multi-keyword search, and achievement of data and search query privacy. Contrary to other works, our multi-user access specifically refers to supporting numerous authors (or data owners) and readers (or data users) at the same time, as well as the distribution system while it is being implemented. Additionally, by implementing a multi-server architecture in the searching and testing process, search queries are handled by some parallel servers to speed up response time and balance workload, and at the same time, keyword guessing attacks from the cloud storage server are successfully resisted. Additionally, the searchable cipher language and the trapdoor are expertly crafted to arrive at a consistent size. Tables are used to compare our plans to the ones that are already in existence. I evaluate the computing and communication capabilities of cloud providers and internal servers based on the hybrid model of our scheme of the two keywords of the process.

Related work

Data will give multiple person authority based on data access will be done in that it has data owner, data user, authority (cloud provider), and Key generation center. In the process data, an owner will upload the file in the cloud before the process is done AES algorithms apply data will be secure in the cloud storage. Song et al. [1] proposed SSE. They presented a sequential scan technique using block cipher and steam cipher procedures to locate the target word WI. However, their strategy's search time is linear with document length. In the cloud lo, data will be used them users will get access. First Users' registration will be done directly they will not log in so they want to be login means the cloud provider needs to give access to them. After they give access to them then only they will log in to the process. They want a file to search them after searching their files will not be visible then they will be in an unreadable format will be available. „. Abdal et al. [8] provided a generic construction of searchable encryption from anonymous IBE (AIBE), formalizing anonymous IBE (AIBE). The unreadable data will be using it does not visible. The film wants to be visible means it needs the key which means key submission will be present. Key submission wants to give means the Key generation center will be a mediator which means a third party in the process. The process has a key generation center will be present they will accept the request then it will generate the key to give to the cloud. The cloud will give the key through the mail of the process. So based on the key normal of the base paper data will access them but coming to future work here data access will be done time taken will be done of the process which means one by-one login means it has time taken to process will happen of process because the key generation wants to accept them then the user will be irritated because of the time is taken process. Secure indexes were introduced by Goh [2]. He designed a safe index that could speed up the server's search. He created semantic security against adaptively selected keyword attack (IND-CKA) security paradigm for indexes initially. Whether the application wants to succeed we need them it should be easy for a user which means in future work KGC will be deleted them so that it has four moduli of the process. In the process, we have internal servers that are there which means distributing when will upload the files in the cloud. The cloud data files are to be distributed and it will store the internal servers which means internal servers 1, and 2,3 are present. So the data want to secure while we uploaded the cloud it will store the internal server will be stored after storing the data file then it will give to the user it will enough in that don't need a mediator because a mediator will key to an unknown person in that data will be a loss. The mediator at one time will be genuine and at times they will be fake so we did not trust the mediator. So that this type of fake doesn't happen again so we did not depend on them in the communication of what is happening cloud to an internal server, internal server to a user of the process no need to access the key generation center Searchable Encryption (SE) is a concept that was introduced in [3 It was divided into two groups: Public key encryption with keyword search (PEKS) and Searchable Symmetric Encryption (SSE) [4]. SSE progresses from the prototype of sequentially scanning the cipher text stream without any index aside [5] to several sophisticated structures [5], [6], and [7] with delicate encrypted indexes to significantly speed up the search operation. Several multi-keyword search support techniques have been presented in the literature [9], [10], [11], [12], and [13]. Their implementations largely rely on SSE or broadcast encryption [14]. Cloud to accept generation then go to the internal server it will generate key it will send to the mail of the user. The Key will be unique will become and should not be fake the key to the process

4. Proposed Methodology

The system in our proposed design is made up of the following parties: Data Providers, Request Users, Cloud Providers, and Internal Servers. see Fig. 1.

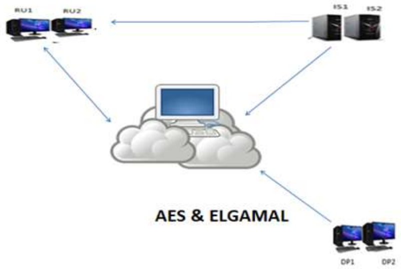
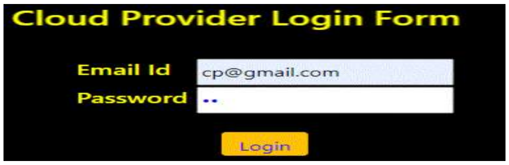


Figure 1. AES and ElGamal Encryption process

Cloud Provider (CP)

The cloud has been adopted in various applications. The cloud is a combination of multiple servers it stores the documents, files, images, and many other files that can be stored in the cloud[18] it is considered an interesting source of computing and storage resources for scientific applications. It corresponds to searchable cipher texts that Data Providers have submitted. With the help of ISs, it can handle search queries and produce keys that are sent to users' email addresses. Users may then use these keys to access and download files belonging to users of the process.



Cloud Provider Login Form

Email Id cp@gmail.com
Password ••

Figure 2. Cloud Provider Login form

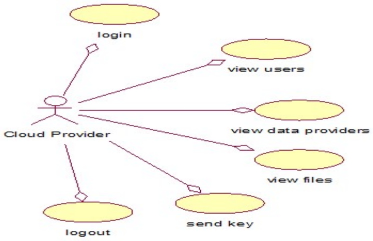


Figure 3. Cloud Provider diagram

Data Providers (DP)

For the Data Provider first, we need to do new registration in that we fill in our details then we submit them then login in data provider it doesn't log in then login into the cloud provider login in that data provider is there a cloud need to accept the details then logout CP. Then login in DP [19] DP are separate methods used in test functions in that upload file in that file name parameter servers and algorithms then upload file then the cloud has to accept the request then it will send to IS then generate a key to the users of the process. Data providers can generate based on the secret and public keys, as well as the public It keeps the documents with the searchable cipher text on the CP in order of keyword searchability.

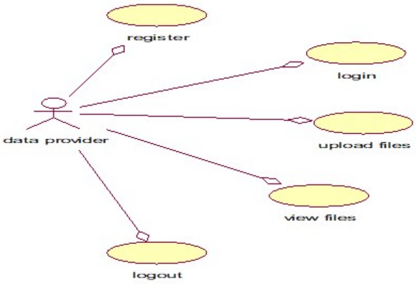
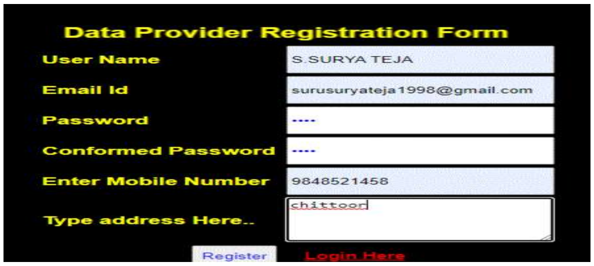


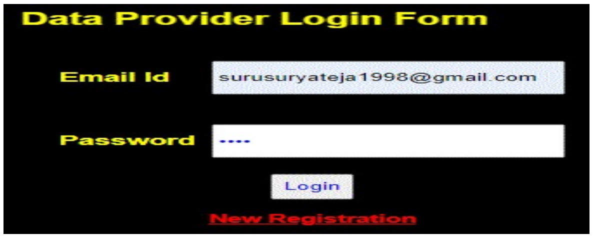
Figure 4. Data Provider diagram



Data Provider Registration Form

User Name	S.SURYA TEJA
Email Id	surusuryateja1998@gmail.com
Password	****
Conformed Password	****
Enter Mobile Number	9848521458
Type address Here..	chittoor

Figure 5. Data Provider registration form


Data Provider Login Form

Email Id: surusuryateja1998@gmail.com

Password: ····

Figure 6. Data Provider login form

Internal servers (IS)

An internal server is an organization of the cloud because it is a cloud combination of multiple servers of them. It will give guidance to the cloud like the Alexa tool of the process. Their implementations largely rely on SSE or broadcast encryption [20] It can deal with a search request. I can be created as a server in a process organization. It can generate a key for the user. The key sent by the user mail based on the key user can access the cloud of the process.

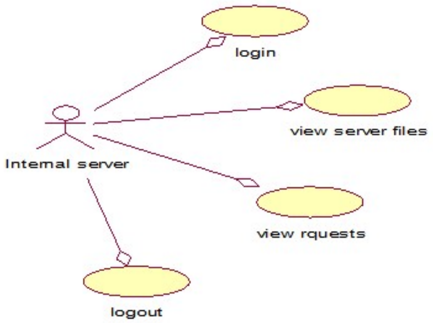
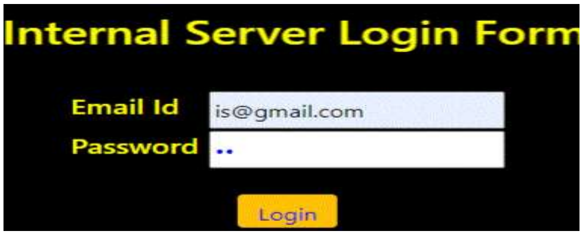


Figure 7. Internal Servers diagram


Internal Server Login Form

Email Id: is@gmail.com

Password: ··

Fig. 8. Internal Servers login form

Request Users (RU)

The user wants to register and then login into the cloud provider then the user can search file [17] it controls by a workflow to make sure it is managed according to a defined process. which file does a user want it is in encryption form then the user need readable form then user want the key to generating by the internal server of the process then user access in the cloud. Each user can generate Depending on the DP, both a private and public key.

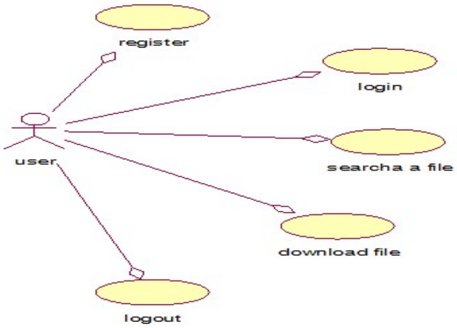
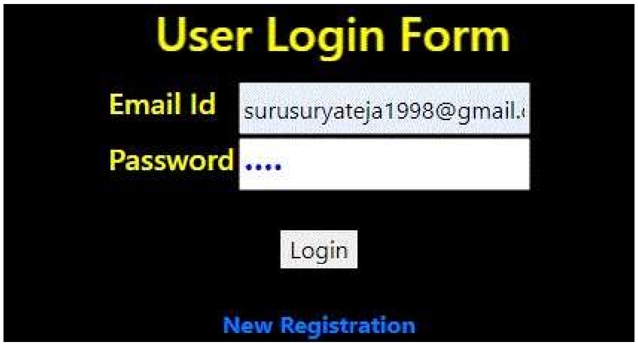


Figure 9. Request Users diagram



User Login Form

Email Id surusuryateja1998@gmail.(

Password ••••

Figure 10. Request Users Login Form

Design Goals

We created the new searchable encryption to meet the functional and security requirements of the process:

i) **Data security**: CP is unable to learn anything about the encryption of the data or keywords that DP has uploaded

ii) **Privacy of Query**: CP is not permitted to find out what keywords In an RU looking for

iii) **Multi-Keyword searches**: these require permission. From a single keyword query, RU is allowed to run both single- and multiple-keyword searches.

iv) **Short Ciphertext and Trapdoor:** The number of keywords has no bearing on the size of the ciphertext and trapdoor, which is fixed.

v)Multi-User Access: The system enables several DPs to offload their data resources to the cloud and multiple RUs to search the same set of data, resulting in a multi-writer/multi-reader environment.

vi) **Access Patterns Hiding**: Search results are hidden from CP, including the identification of documents that match the query.

5. AES and Elgamal Encryption process

The cloud computing page has come it is like an Html page in that it has a homepage, Data provider, User, internal server, and cloud providers are present. In that first, go to the data providers in the DP we need to new registration to fill in all details and then submit the details then it came to the login page we have to log in it doesn't work then go to the cloud provider then login in the cloud in there is a homepage, data provider, user, logout view data provider, view user request of the process. [15] This algorithm has its particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world Then we have to go to the data provider in that when we submit the details are present then there is accept /reject are there we need to accept them. Then go to the data provider login after login in data provider it has the upload file, and the view file sees the fig. 10. In we open the upload file it has some columns are there is a file name, parameter, servers, algorithms, and upload file after doing the process of upload the file then go to view a file in that we see the what we upload details are present. Later finally log out from the data provider.

User process in that first we need to do new registration of the user fill in the details of the user then submit the details then it comes to the login page. Then login the user we were given the details which mean the user id and password of them. On the user page, it has a search file and a download file. Go to the search file in which it has asked which search will show the details of that file then send request option is there .it will send to the cloud provider to users. then go to CP login after login there is a view user request column is there opened then accept it. there is a message that is request accepted and information shared by the internal server.

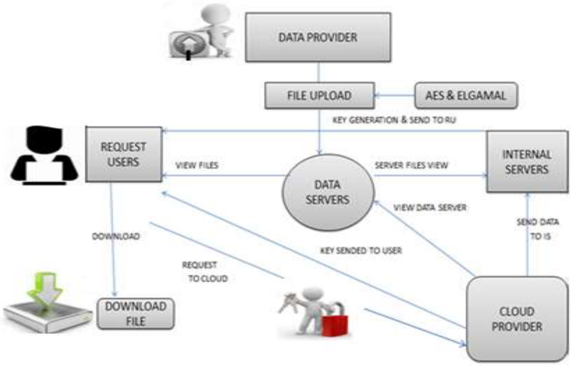


Figure 11. Block Diagram of AES and ElGamal Encryption process

The internal server is key generated & sends to RU of the process. Then login to the internal server that has view server details, request files and log out. In that we go to the request files where user details are present of them there is an option that is generally a key in the action columns of the process the generate key click it then the key will go to a user's mail ID. The user verifies the mail copies the OTP then the IS to be logout of them. To go to the user page means the login page then the user login goes to the download file and there is a download option present click it will ask for the OTP there paste it view data click it it will show the file that we want them of the process then download the file and open it of them.

5.1 Algorithms

This paper represented the hybrid model that is a combination of the two algorithms, there are AES and ElGamal algorithms of the process we explain detailing the process of them

5.1.1 Advanced Encryption Standard (AES) Algorithm

- The United States picked the symmetric block cipher known as 2001, the Advanced Encryption Standard to safeguard secret information.
- AES is a block cipher algorithm that may be used for both encryption and decryption.
- AES has an input array, state array, and key array.

- The number of rounds is dependent on the key length and ranges from 128 bits keys to 12 rounds.

The size of the key is 128/192/256 bits. 14 rounds of the procedure, 256-bit key.

Step for AES Algorithm

- The block data (plain text) and the starting state key with the initial round key added should be used to initialize the state array.
- The set of round keys should be derived from the encryption key.
- Execute the first Nine rounds of state interference
- the eleventh and last round of state manipulation;
- Copy the final state of the encryption data (cipher text)

5.1.2 Elgamal Algorithm

ElGamal algorithm is a public key cryptosystem it uses asymmetric key encryption it deals with communication between two parties and encryption the message of them.

The following cryptosystem, which uses primitive roots, was developed in 1985. The system's security is based on how challenging it is to solve the Problem with discrete logarithms r x a (mod p) or x = Indr (a). As demonstrated, looks to be essentially random as a function of a, making it a good option for a basis of security

Every user of the ElGamal system: choose one of its primitive roots r and a (big) prime p. selects and calculates a The encryption key KE = is made available by the (secret) decryption key KD = k with 2 k p 2. 0 a p 1. a = r k (mod p) (p, r, a).

Be mindful that to establish KD = k, an unauthorized individual would have to complete the incredibly difficult operation of computing indr(a). To transmit a message to the user whose public key is KE =, the sender transforms her message M into numerical blocks B of size p 1. (p, r, a).

Determines 0 C1, C2 p1, C1 r j (mod p), and C2 Baj (mod p) for each block B., using a J with (secret) 2 j p 2. If necessary, Each block can change the value of the key j. sends the couples (C1, C2). By multiplying by a j, the message block was encrypted, and the exponent j was concealed

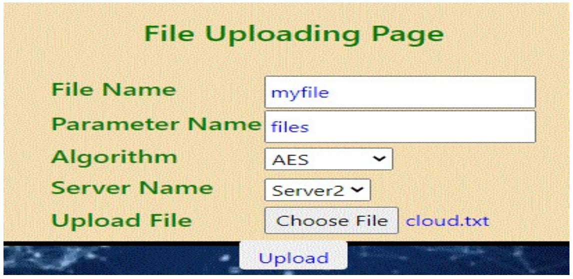
Even though it is well known that KE = (p, r, a), the computation of Indr is necessary to extract j from C1 (C1). However, the intended recipient computes B j without being aware if they are aware that KD = k. The Theory of Fermat is applied within the last line, C2C p1k. 1 (Baj)(r j) p1k (mod p) B(r KJ r j(p1)k (mod p) B(r p1) j (mod p) (mod p),

Since using public key cryptography encryption keys do not keep It is essential to be able to keep things verify who sent any communication. [16] This article explores ElGamal public key encryption algorithm that is put into practice into information transmission that indicates that it will display the numbers repeatedly done on the data provider Any participant in an ElGamal cryptosystem can add a digital signature to any communication using their public and private keys. Using their own public key KE =, the sender of the message determines the exponent j and calculates c r j (mod p) (p,r, a). The linear congruence JD + kc B (mod p 1) for the first plaintext block B is then solved by the sender using the EA

where the sender's secret decryption key is KD = k
The digital signature (c, d) is then added by the sender to the encrypted message. Keep in mind that To have computed the secret variables k, j, and B, the sender must have them (c, d). The recipient of the message uses the sender's key, KE = (p,r, a), to determine V1. a c c d (mod p) and V2 r B, which are used to verify the signature (mod p). As long as V1 Equals V2, the signature is valid because of V1 a c c d (r k) c (r j) d r kc+jd r B V2 (mod p).

6. Result Analysis

6.1 AES Algorithm Results:

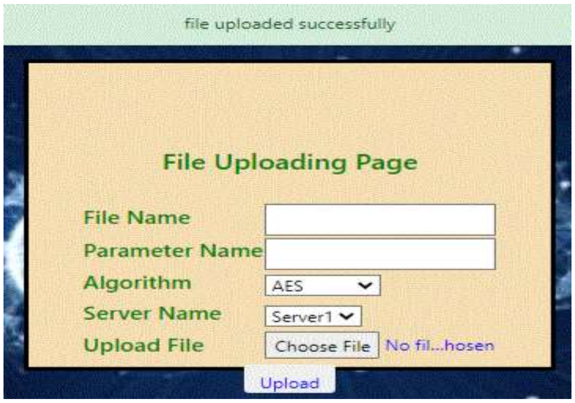


File Uploading Page

File Name	myfile
Parameter Name	files
Algorithm	AES
Server Name	Server2
Upload File	Choose File cloud.txt

Figure 11: File Upload Page in the cloud

The above fig 11, users write a file name (file) and a parameter name (what type of file is this?), then algorithms (there are options AES and Elgmal; we select AES algorithms), then server name (it means where they want to save the file), then server 2 and upload file (we select and upload them).



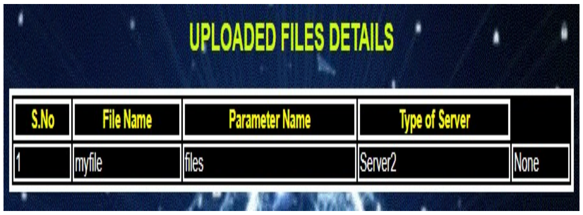
file uploaded successfully

File Uploading Page

File Name	
Parameter Name	
Algorithm	AES
Server Name	Server1
Upload File	Choose File No fil...hosen

Figure 12. File Upload Successfully in the cloud

In that case, we uploaded to the cloud the information provided by the data providers. It will be saved in the cloud

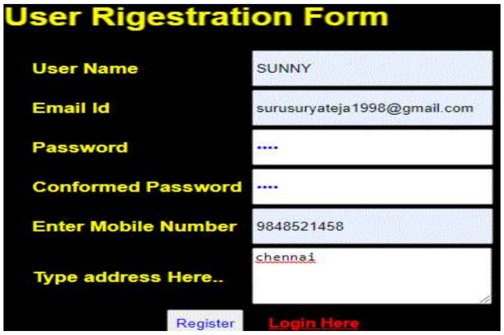


UPLOADED FILES DETAILS

S.No	File Name	Parameter Name	Type of Server	
1	myfile	files	Server2	None

Figure 13. Upload Files Details

The above fig. 13, what we uploaded in data provider in those column view files when opened, will show the table columns like serial no., filename, parameter name, server types, and cipher text of AESA algorithms that are present in the process.

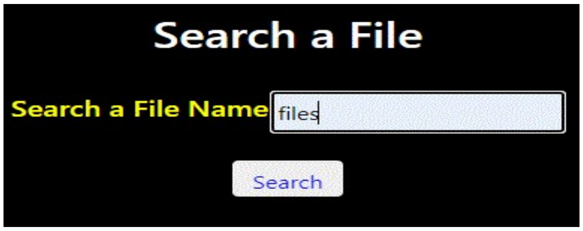


User Rigestration Form

User Name	SUNNY
Email Id	surusuryateja1998@gmail.com
Password	••••
Conformed Password	••••
Enter Mobile Number	9848521458
Type address Here..	chennai

Figure14. User Registration Form in the cloud

In the above fig. 14, there are six columns: username means the person's name, email id means the person's email id, passwords mean to write new passwords like strong passwords, and conform passwords mean what the user has written in the password will be presented, mobile no. means to write down the user's address, and then register it will present the process's login page.

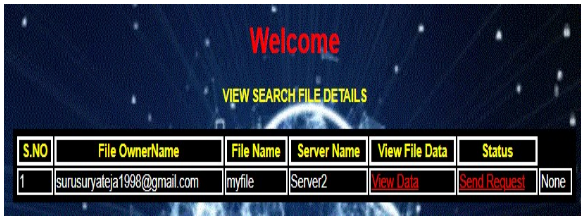


Search a File

Search a File Name: files

Figure 15. Search A File in the cloud

The above fig. 15, the search file column is present in the user page in which it was opened in the above figure, and in that search, a file name column is present in which you type the name of the file you want, click the search button, and the process begins



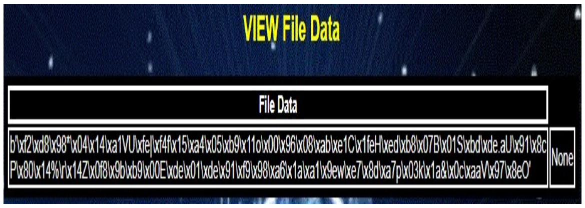
Welcome

VIEW SEARCH FILE DETAILS

S.NO	File OwnerName	File Name	Server Name	View File Data	Status	
1	surusuryateja1998@gmail.com	myfile	Server2	View Data	Send Request	None

Figure 16. View Search File in the cloud

In the above fig 16, after clicking the search file, it will display the above figure, which means that the serial number, file owner name, file name, server name, view data status, and none mean the cipher text of the AESA algorithms of the process.

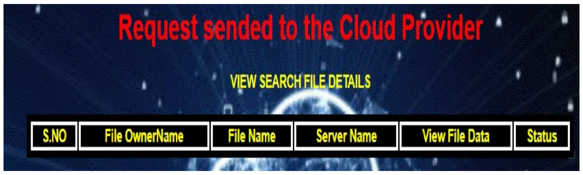


VIEW File Data

File Data	
b'\xf2\xd8\x98*\x04\x14\xa1VU\xfe|\xf4f\x15\xa4\x05\xb9\x11o\x00\x96\x08\xab\xe1C\x1feH\xed\xb8\x07B\x01S\xbd\xde.aU\x91\x8cP\x80\x14%\r\x14Z\x0f8\x9b\xb9\x00E\xde\x01\xde\x91\xf9\x98\xa6\x1a\xa1\x9ew\xe7\x8d\xa7p\x03k\x1a&\x0c\xaaV\x97\x8eO'	None

Figure 17. View File Data in the cloud

In the above fig. 17, in the data of the above page, there is an option to "view data," which means that if opened, it will display the above fig, which is encrypted in the process's AES algorithms.



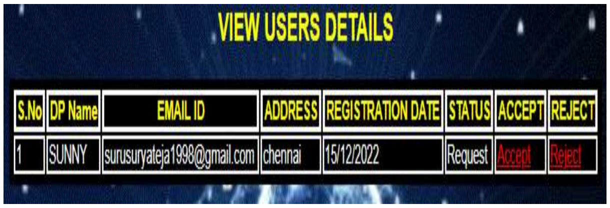
Request sended to the Cloud Provider

VIEW SEARCH FILE DETAILS

S.NO	File OwnerName	File Name	Server Name	View File Data	Status

Figure 18. Request Send to the Cloud Provider

In fig. 18, we need to send the request to the cloud, then log out, visit the cloud provider, and accept the request in the cloud process

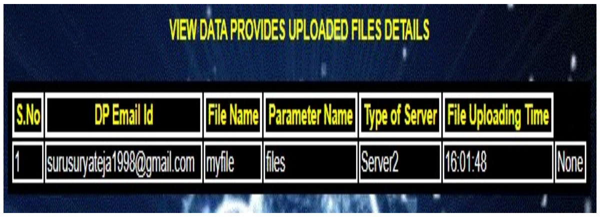


VIEW USERS DETAILS

S.No	DP Name	EMAIL ID	ADDRESS	REGISTRATION DATE	STATUS	ACCEPT	REJECT
1	SUNNY	surusuryateja1998@gmail.com	chennai	15/12/2022	Request	Accept	Reject

Figure 19. View User Details in the cloud

Above fig 19, the cloud in the above figure has columns for user request files that are present; we must navigate to the columns to access the data: provider name, email ID, address registration date, status, accept or reject of the process, and so on.

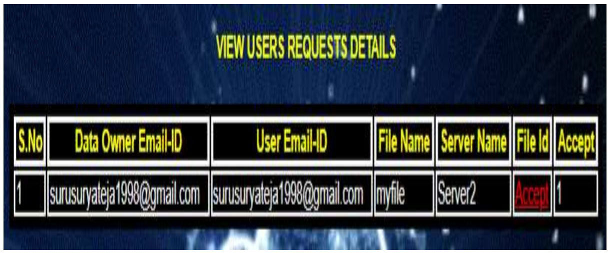


VIEW DATA PROVIDES UPLOADED FILES DETAILS

S.No	DP Email Id	File Name	Parameter Name	Type of Server	File Uploading Time	
1	surusuryateja1998@gmail.com	myfile	files	Server2	16:01:48	None

Figure 20. View Data Provider Uploaded Files Details

Above fig 20, the cloud in the above figure has another column that says "view data provider files," and after opening the file, the following information is displayed: data provider email id, file name, parameter name, type of server file uploaded time, and the AES encryption process.

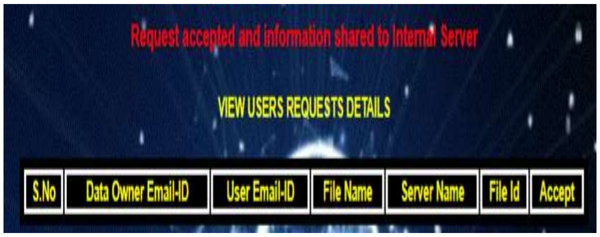


VIEW USERS REQUESTS DETAILS

S.No	Data Owner Email-ID	User Email-ID	File Name	Server Name	File Id	Accept
1	surusuryateja1998@gmail.com	surusuryateja1998@gmail.com	myfile	Server2	Accept	1

Figure 21. View User Request Details in the cloud

In the above fig 21, the cloud provider that has the view user request file column is present after opening it. It will show the table column in that data: owner email id means write email id, user email id means user mail id, filename means which file is uploaded, server name means which server uploaded the file, and file id means to accept, or reject are present in the process.



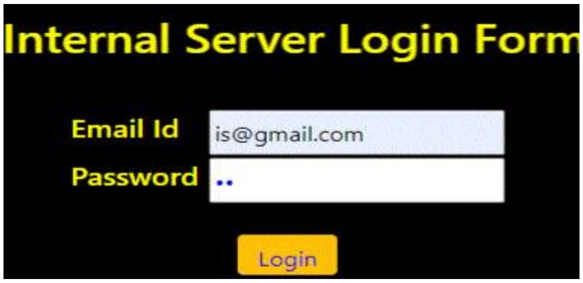
Request accepted and information shared to Internal Server

VIEW USERS REQUESTS DETAILS

S.No	Data Owner Email-ID	User Email-ID	File Name	Server Name	File Id	Accept

Figure 22. Request Accepted and Information Shared to Internal Server

Above fig 22, there is a column file id in the above fig that says accept or reject, then accept them to the cloud, then it will give the message "Request accepted, information shared with internal server," then log out of the cloud provider and go to the internal server.



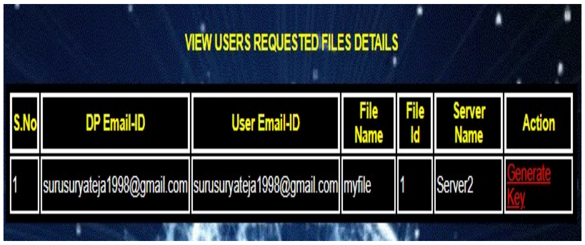
Internal Server Login Form

Email Id: is@gmail.com

Password: ••

Figure 23. Internal Server Login Form in the cloud

Above fig 23, the internal server in the above figure is one of three servers in the process; once the cloud has accepted the files and details of the users, it will generate the key in the process's internal server.

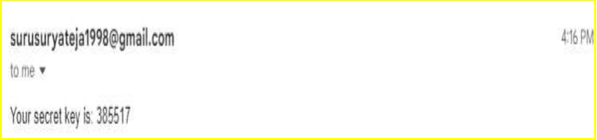


VIEW USERS REQUESTED FILES DETAILS

S.No	DP Email-ID	User Email-ID	File Name	File Id	Server Name	Action
1	surusuryateja1998@gmail.com	surusuryateja1998@gmail.com	myfile	1	Server2	Generate Key

Figure 24. View Users Requested Files Details in the cloud

In the above fig 24, the internal server has two columns: request file details and view server details, which are present because we needed to open request files. It will show the view user request file details in that the data provider email id wants to write them, the user email id wants to write them, and the file name means which file the user wants them. The server name indicates which server is uploading them, and the action indicates that it needs to generate a key for the process's user mail, then click it. It will generate a key.

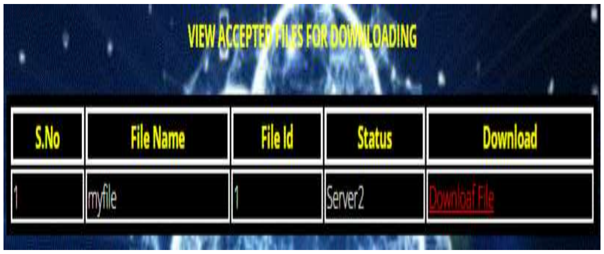


surusuryateja1998@gmail.com 4:16 PM
to me ▾

Your secret key is: 385517

Figure 25. Key in Mail id

In the above fig 25, the key it has sent by the internal server to the user mail id then copies the key then uses it for the download file of the process.

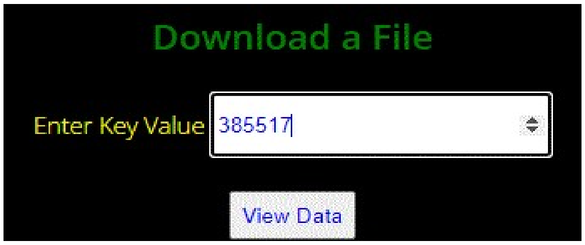


VIEW ACCEPTED FILES FOR DOWNLOADING

S.No	File Name	File Id	Status	Download
1	myfile	1	Server2	Downloaf File

Figure 26. View Accepted Files for Downloading in the cloud

In the above fig 26, after obtaining the key, navigate to the user login page, and then to the process download file in that table column.

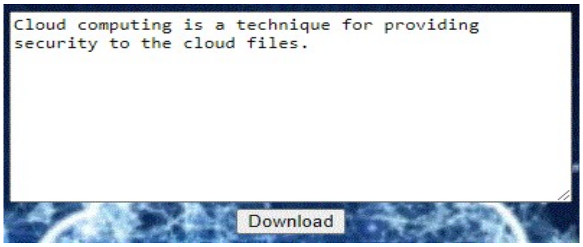


Download a File

Enter Key Value: 385517

Figure 27. Download the File in the cloud

In the above fig 27, clicking the "download file" button opens the enter key-value box as "download a file," and after copying the key present in the box, we click the "view data" button to see the process.

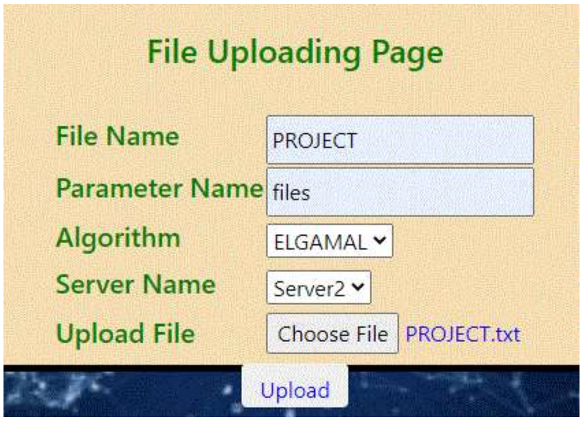


```
Cloud computing is a technique for providing
security to the cloud files.
```

Figure 28. Output of AES Algorithm

After clicking on "view data" in the preceding figure, the output of the process's AES algorithms will be displayed.

6.2 Elgamal Algorithm Results:

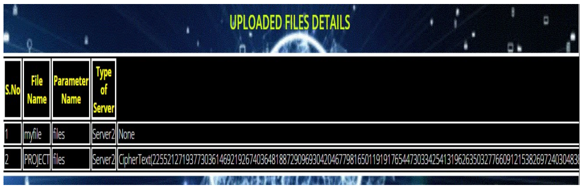


File Uploading Page

File Name	PROJECT
Parameter Name	files
Algorithm	ELGAMAL
Server Name	Server2
Upload File	Choose File PROJECT.txt

Figure 29. File Uploading Page in Elgamal in the cloud

In the above fig. 29, users write a file name, which is my file, and a parameter name, which is what type of file this is, and then algorithms, which are AES and ElGamal, which we select, then server name, which is where they want to save the file, then server 2, and upload the file, which is where we choose the file and select and upload them.

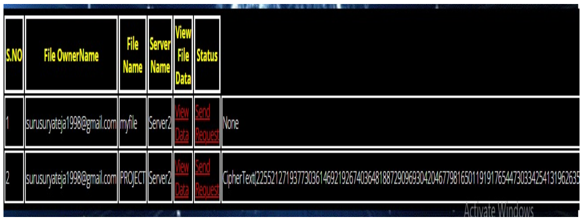


UPLOADED FILES DETAILS

S.No	File Name	Parameter Name	Type of Server	
1	myfile	files	Server2	None
2	PROJECT	files	Server2	CipherText(2255212719377303614692192674036481887290969304204677981650119191765447303342541319626350327766091215382697240304838

Figure 30. Upload Files Details

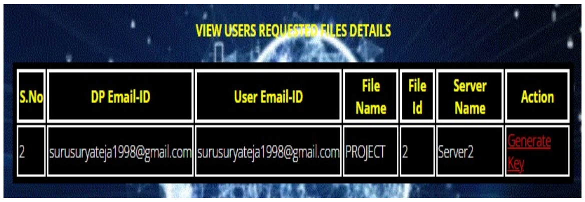
In the above fig. 30, It contains both AES and ElGamal files of the process; file names such as "my file" is written in them, and parameter names such as file names and server names are written; AES encryption form is "none," and Elgamal encryption form is cipher text such as some numbers are present in the process.



S.NO	File OwnerName	File Name	Server Name	View File Data	Status	
1	surusuryateja1998@gmail.com	myfile	Server2	View Data	Send Request	None
2	surusuryateja1998@gmail.com	PROJECT	Server2	View Data	Send Request	CipherText(22552127193773036146921926740364818872909693042046779816501191917654473033425413196263 5

Figure 31. Search File in the cloud

In the above fig 31, It is on the user page, and it has a table format of AEs and ELGAML encryption forms. In AEs, there will be a binary form of ciphertext, and in ELGAML, there will be a number form of ciphertext. I need to click the send request button, and it will go to the cloud provider and accept them. It will show requests accepted and information shared by the internal server, then go to the internal server of the process.

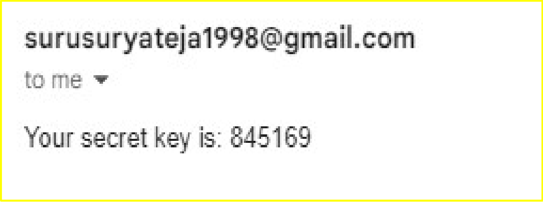


VIEW USERS REQUESTED FILES DETAILS

S.No	DP Email-ID	User Email-ID	File Name	File Id	Server Name	Action
2	surusuryateja1998@gmail.com	surusuryateja1998@gmail.com	PROJECT	2	Server2	Generate Key

Figure 32. View User Requested Files Details

In the above fig.32, The requested files will be present on an internal server page, and there is a table column with the data provider email id, user email id, file name, file id, server name, and action. In that key action, the action will be performed, and the file will be opened. It will generate a key and send it to the user's email address

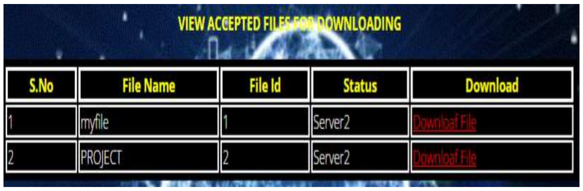


surusuryateja1998@gmail.com
to me

Your secret key is: 845169

Figure 33. Key in Mail id

In the above fig.33, the key it has sent by the internal server to the user's mail id, copy the key, and use for the download file of the process.

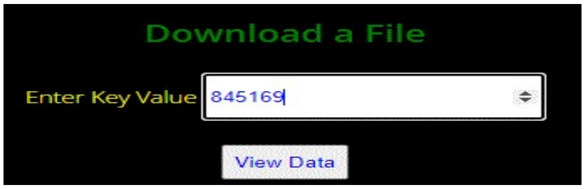


VIEW ACCEPTED FILES FOR DOWNLOADING

S.No	File Name	File Id	Status	Download
1	myfile	1	Server2	Downloaf File
2	PROJECT	2	Server2	Downloaf File

Figure 34. View Accepted Files for Downloading

In the above fig. 34, This will be visible on the user page in the form of a download file column, an opened file column, and a table column of AEs and Elgamal with file name, file id, status, and download. In the download file, open the download file of the process.

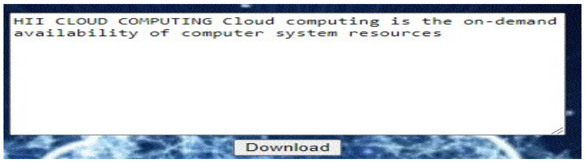


Download a File

Enter Key Value: 845169

Figure 35. Download the File in the cloud

In the above fig. 35, The "enter key value" box appears after we copied the key from the box and clicked on "view data" for the process after clicking on the "download file" button.



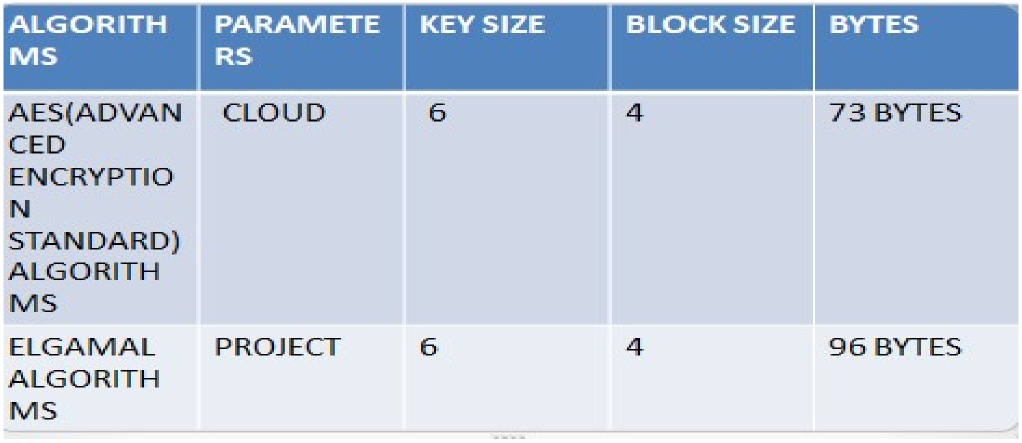
```
HII CLOUD COMPUTING Cloud computing is the on-demand
availability of computer system resources
```

Figure 36. Output of ElGamal Algorithms

In the above fig. 36, after clicking on "view data" in the preceding figure, the output of the process ELGAMAL algorithms will be displayed.

6.3 Tables of Algorithms

Table – 1: Comparison of AES and ELGAMAL algorithms



ALGORITHMS	PARAMETERS	KEY SIZE	BLOCK SIZE	BYTES
AES(ADVANCED ENCRYPTION STANDARD) ALGORITHMS	CLOUD	6	4	73 BYTES
ELGAMAL ALGORITHMS	PROJECT	6	4	96 BYTES

7. Conclusion

To formalize AES and ElGamal algorithms and ensure the security of cloud data, I established a new searchable encryption scheme with our innovative subset decision methods. I created a practice in distribution architecture and demonstrated that AES and ElGamal algorithms are used to satisfy our suggested security criteria. In addition to the scheme, it has appealing features like constant-size trapdoors, cipher text, and multi-keyword support. It also hides the search patterns and access patterns, when searching it supports multiple writers and readers. The comparison of the schemes is evaluated and the results show that our scheme beats alternative options in the terms of total performance. I show that the HYBRID MODEL (AES & ElGamal) secures data through process-based interaction and computation between CP and IS.

Reference

[1]X. Liu, G. Yang, W. Susilo, J. Tonien, X. Liu, and J. Shen, "Privacy-Preserving Multi-Keyword Searchable Encryption for Distributed Systems," IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 3, March 1, 2021, pp. 561–574, DOI: 10.1109/TPDS.2020.3027003

[2] "Public key encryption with keyword search," in International conference on the theory and applications of cryptographic techniques, 2004, pp. 506–522. D. Boneh, G. Di

[3]. Information Sciences, vol. 403, pp. 1-14, 2017. Q. Huang and H. Li, "An efficient public-key searchable encryption system secure against inside keyword

[4]. An effective privacy-preserving outsourced calculation toolkit with multiple keys is described by X. Liu, R. H. Deng, K.-K. R. Choo, and J. Weng in IEEE Transactions on Information Forensics and Security, vol. 11, no. 11,

[5Practical algorithms for searches on encrypted data, D. X. Song, D. A. Wagner, and A. Perrig, Proc. IEEE Symp. Security and Privacy, 2000, pp. 44–55.

[6]. IACR Cryptology ePrint Archive, vol. 2003, 2003, art. no. 216, E. Goh, "Secure indexes."

[7]. "Worldwide personal cloud storage consumers and users from 2014 to 2020 (in millions)," available at https://www.statista.com/statistics/638593/global-data-center-storage-capacity-cloud-vs-traditional/.

[8]. Dual-server public-key encryption with a keyword search for secure cloud storage, IEEE Trans. Inf. Forensics Secure., vol. 11, no. 4, pp. 789-798, R. Chen, Y. Mu, G. Yang, F. Guo,

[9]. Processing Analytical Queries over Encrypted Data, Proc. VLDB Endow., vol. 6, no. 5, pp. 289–300, S. Tu, M. F. Kaashoek, S. Madden, and N.

[10 B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 262–267,

[11]K. Huang, R. Tso, and Y.-C. Chen, "Somewhat semantic secure public key encryption with filtered-equality-test in the standard model and its extension to searchable encryption," Journal of Computer and System Sciences, vol. 89, pp. 400–409,

[12]. "Off-line keyword guessing attacks against current public key encryption with keyword search algorithms," in Autonomic and Trusted Computing, International Conference, ATC 2008, Oslo, Norway, Proceedings, pp. 100-105, by W.C. Yau, S.H. Heng, and B.M. Goi.

[13[Q. Tang, Public Key Encryption Schemes Supporting the Equality Test with Different Granularity of Authorization, IJACT 2 (2012)

[14]. Susilo, Willy; Kim, Hyun-Jeong; Rhee, Hyun Sook Stop keyword guessing attacks on your searchable public key encryption system. 237–243 in IEICE Electronics Express, 6(5).

[15]https://www.researchgate.net/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data

[16] Wu, Zengqiang; Su, Di; Ding, Gang (2014). [IEEE 2014 International Conference on Mechatronics and Control (ICMC) - Jinzhou, China International Conference on Mechatronics and Control (ICMC) - ElGamal algorithm for encryption of data transmission. , (), 1464–1467.

[17]https://www.researchgate.net/publication/321348098_Cloud_Computing_A_Survey_on_Service_Providers

[18] Bubak, M.; Kasztelnik, M.; Malawski, M.; Meizner, J.; Nowakowski, P.; Varma, S. International Symposium on Cluster, Cloud and Grid Computing (CCGrid) - Delft International Symposium on Cluster, Cloud, and Grid Computing - Evaluation of Cloud Providers for VPH Applications.

[19] Fiat and M. Naor, "Broadcast encryption," in AnnualInternational Cryptology Conference, 1993, pp. 480–491.

[20] K Janshi Lakshmi and Prof. G Sreenivasulu, "A Review On FPGA Based Design of Advanced Encryption Standard (AES) Cryptography Secure Algorithm", i-manager's Journal

on Communication Engineering and Systems, Volume 10. No. 1 January - June 2021, ISSN - 2277 – 5102, p-p: 30 – 40.

[21] A Framework for the Semantic Composition of Web Services Handling User Constraints - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/User-request-service-description-handling-user-requests_fig3_221587054 [accessed 12 Dec 2022]