International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

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

ABSRACT

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 can 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 is becoming increasingly popular among both personal and individual users. The cloud computing procedure will have five columns. Before the page displays and we are required to log in since access is supplied by cloud services, we must first contact the data provider and complete a new registration in which we submit our information, after which we must proceed to the CP [17]. The study covers clouds, cloud storage, and service providers based on many characteristics such as pricing, maximum storage limit, and subsequent data security.

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, the registration date means when the user registered, 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 proceed to the data provider.

When the task is completed, the data provider will display the successful page next to the person's name. The data provider includes columns for the homepage, viewing files, and uploading files. Upload files indicate that the file name, parameters, algorithms, servers, upload files, and upload options will all be displayed on the file upload page. Here, "file name" refers to files; it can be "files" or "my files," "server" refers to the three cloud servers: server 1, server 2, and server 3, and "upload files" refers to the choose file option; we will select the files we want to upload and click the upload button.

It displays the uploaded file, and then we click to view files to examine the file name, server type, and

encryption form to determine what that implies.

AES algorithm [15]. This technique has a unique structure for encrypting and decrypting sensitive data and is used in hardware and software all around the world, signaling that they will display no format (binary). ELGAMAL [16] is a public key encryption technique that is used to transmit information. It means that it will display the numbers entered repeatedly on the data provider.

Come to the homepage, then to the user page where we wish to register users, and it will display the registration page for the procedure. Fill in the users' information and then click submit. But it won't, because the cloud wants to accept the information. When there is a user request column, click on it to view the user's information; then click Accept to accept the information. Go to the user page, log in as that user from the home page, search for files, and download them. Search file implies that we want to search what we upload in DP files.

It will display the file owner's name, file name, server name, view file contents, and status (if a request form is provided), followed by the send request, which will display the request sent to the cloud. Go to the cloud login page, where there is a column for user requests files; click it in the data owner email address, user email address, file name, server name, file id, and accept. It will signal that the request was accepted and that data was transferred to the internal server. Then go to the internal server page, where an internal server login page will appear.

It has a homepage, displays server information, requests files, and allows you to. Then navigate to the requested files, which include an email ID, user email ID, file name, file ID, server name, and action. It has taken action by creating a key, which is now visible in columns. Then the process of generating the key will load a page after the OTP is sent to the user's email; copying it will display the key sent to the user; there is a "download file" column. That file includes the file name, ID, status, and download. It has opened the file from that download.

The download file contains the key values received in the mail, such as "OTP". It will save the downloaded file to a download folder. The file is opened in Notepad, and we can see the process file; therefore, we will upload multiple files and download multiple versions of the process.

CONTRIBUTION

In this work, we provide a new public-key searchable encryption system that relies on a hybrid architecture to address security, privacy, and functionality problems. The method can be used on multiple specified servers to allow the public key cloud storage server to perform a multi-keyword search over encrypted data while protecting privacy in distributed contexts with multiple data writers and users. Our technique, Searchable Encryption, is based on a productive, externally determined structure with several keys for privacy protection.

To determine if one input set is a subset of the other, I develop novel subset determination algorithms. The provided techniques formed the basis for the multi-keyword search feature in a two-server architecture. It will be useful for various operations that require testing on private subsets.

The fundamental approach of our scheme's subset choice processes. The suggested plan provides support for multiple users, multi-keyword search, and data and search query privacy.

Unlike other works, our multi-user access focuses on supporting several authors (or data owners) and readers (or data users) at the same time, as well as the distribution system while it is being developed. Furthermore, by including a multi-server architecture into the searching and testing process, search queries are handled by certain parallel servers to speed up response time and balance burden, while keyword

guessing attacks from the cloud storage server are effectively avoided. Furthermore, the searchable cipher language and trapdoor are precisely designed to achieve a consistent size. Tables are utilized to compare our plans to those that currently exist.

I examine the processing and connectivity capabilities of cloud providers and internal servers using the hybrid model of our process's two keywords.

RELATED WORK

Data will be granted numerous levels of authority based on data access, with data owners, data users, authorities (cloud providers), and a key generation center. In the process data, an owner will upload the file to the cloud before the procedure is completed. AES algorithms ensure that data is secure in cloud storage. Song et al. [1] suggested SSE. They demonstrated a sequential scan strategy that employed block cipher and steam cipher procedures to discover the target word WI. However, their strategy's search time is proportional to document length. Data will be stored in the cloud, and users will have access to it.

First, users will register directly; they will not log in, so if they wish to log in, the cloud provider must provide them access. After they grant them access, only they will be able to log in to the process. They want to search for a file. If their files are not accessible, they will be offered in an unreadable format. ,. Abdal et al. [8] formalized anonymous IBE (AIBE) by constructing a generic searchable encryption from it. The illegible data will not be visible. The film's desire to be seen necessitates the use of the key, which implies that key submission will occur.

Key submission wants to give means that the Key generation center will act as a mediator, or third party, in the process. The procedure includes a key generation center, which will take the request and generate the key to send to the cloud. The cloud will provide the key via email during the process.

So, based on the key normal of the base paper, data will be accessed, but in the future, data access will be done in the time taken by the process, which means one-by-one login means it will take time to process because the key generation wants to accept them, and the user will be irritated because of the time taken process. Goh [2] introduced secure indexes. He created a secure index to speed up the server's search. Initially, he developed a security paradigm for indexes called semantic security against an adaptively selected keyword attacks (IND-CKA).

If the application is to succeed, we need them, and they should be simple for the user, which means that KGC will be removed in the future so that the process has four modules. We have internal servers present throughout the process, which means that when the files are uploaded to the cloud, they are distributed. The cloud data files will be disseminated, and they will be stored on internal servers 1, 2, and 3.

So the data that we wish to secure while uploading to the cloud will be stored on the internal server. After saving the data file, it will be given to the user, which will suffice because a mediator will key to an unknown person, resulting in data loss. We didn't trust the mediator because they may be honest at moments and then false at others.

So that this type of fake does not happen again, we did not rely on them in the communication of what is occurring 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 notion introduced in [3]. It was classified into two categories: public key encryption with keyword search (PEKS) and searchable symmetric encryption (SSE) [4].

SSE evolves from the prototype of sequentially scanning the cipher text stream with no index aside [5] to many advanced structures [5], [6], and [7] with delicate encrypted indexes to substantially speed up the

search process. Several multi-keyword search assistance strategies are described in the literature [9], [10], [11], [12], and [13]. Their implementations are usually based on SSE or broadcast encryption [14]. Cloud to accept generation, then proceed to the internal server, which will generate the key and send it to the user's email address. The key will be unique and should not be faked for the process.

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 EIGamal Encryption process cloud provider (CP)

The cloud has been employed in a variety of applications. The cloud is a collection of servers that store documents, files, photos, and a variety of other file types[18]. It is seen as a promising source of computational and storage resources for scientific applications. It corresponds to the searchable ciphertexts that Data Providers have provided. It uses ISs to handle search queries and generate keys that are emailed to users' email addresses. Users can then use these keys to access and download files that belong to other process participants.

Figure 2. Cloud Provider Login form

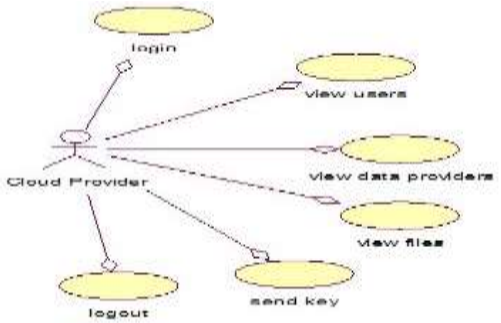

Figure 3. Cloud Provider

Data Providers (DP)

For the Data Provider, we must first complete a new registration in which we provide our information, submit it, and then login into the data provider. If there is a cloud, we must accept the information and

logout of the CP. Then login to 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 must accept the request, then send it to IS, and finally generate a key for the process users.

Data providers can generate depending on the secret and public keys, as well as the public. The documents with searchable cipher text are stored on the CP in order of keyword searchability.

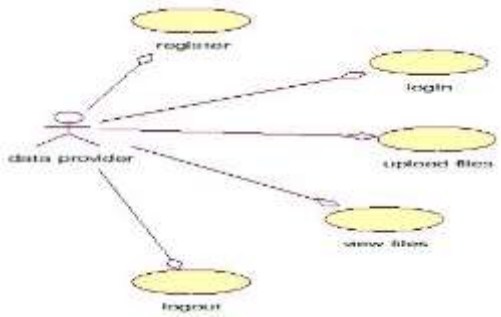

Figure 4. Data Provider diagram

Figure 5. Data Provider registration form

Figure 6. Data Provider login form

Internal servers (IS)

An internal server is part of the cloud because it is made up of numerous servers. It will guide the cloud, similar to the Alexa tool, through the process. Their implementations are usually based on SSE or broadcast encryption [20]. It can handle a search request. I can be configured as a server in a process organization. It can create a key for the user. The key given via email allows the user to access the process cloud.

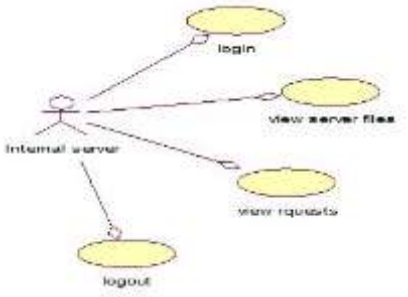

Figure 7. Internal Servers diagram

Fig. 8. Internal Servers login form Request Users (RU)

To search files, the user must first register and login to the cloud provider (reference 17). It is monitored by a workflow to ensure that it is managed in accordance with a predetermined process. Which file does a user want? If it is encrypted, the user needs a readable version. If the key is generated by the process's internal server, the user can access it in the cloud. Depending on the DP, each user can generate a private and public key.

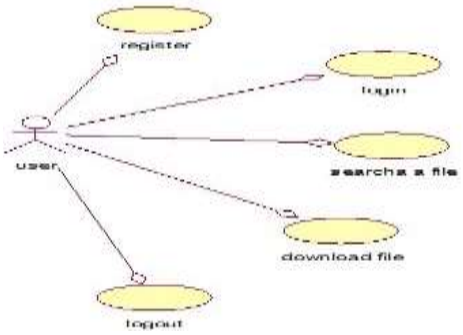

Figure 9. Request Users diagram

Figure 10. Request Users' Login Form

Design Goals

1. We developed the new searchable encryption to suit the process's functional and securityrequirements.
2. Data security: CP cannot access the encrypted data or keywords uploaded by DP.

3. Query privacy: CP cannot determine the keywords an RU is searching for.
4. Multi-keyword searches require permission. RU can perform single- and multiple-keyword searches using a single keyword query.
5. We created new searchable encryption to meet the process's functional and security needs.
   Data security: CP is unable to read the encrypted data or keywords uploaded by DP.
   Query privacy: CP cannot determine the terms an RU is looking for. iii) Multi-keyword searches require approval. RU can run both single- and multiple-keyword searches with a single keyword query.
   Short Ciphertext and Trapdoor: The size of the ciphertext and trapdoor remains constant regardless of the number of keywords used.
   Multi-User Access: The system allows numerous DPs to transfer data resources to the cloud and multiple RUs to search the same set of data, creating a multi-writer/multi-reader scenario.
6. Access Patterns Hiding: CP cannot view search results or identify documents that match the query.
7. AES and Elgamal Encryption process
8. The cloud computing page is similar to an HTML page in that it includes a homepage, data provider, user, internal server, and cloud providers. 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 there is a homepage, data provider, user, logout view data provider,

View the user request for the process. [15] This algorithm has a specific structure for encrypting and decrypting sensitive data and is used in hardware and software all around the world. Then we must go to the data provider, and when we submit the details, there will be an accept/reject option, which we must accept. Then proceed to the data provider login page. After logging in, there is an upload file and a view file that shows Figure 10.

When we open the upload file, we find certain columns such as a file name, parameter, servers, algorithms, and upload file. After uploading the file, we proceed to examine the file and see the specifics of what we uploaded. Later, log out of the data provider. The user process begins with a new registration of the user, where we fill in the user's details, submit the details, and then proceed to the login page.

After logging in, we were provided the user's data, which included their user id and password. The user page includes a search file and a download file. Go to the search file where it asks which search will show the details of that file, and then select the send request option. It will transfer data to the cloud provider for consumers. Then go to CP login. After logging in, a view user request column will appear; accept it. The internal server sends a message indicating that the request has been accepted, and information has been shared.

Figure 11. Block Diagram of AES and ElGamal Encryption process

The internal server generates a key and transmits it to the process's root user. Then, log in to the internal server that contains server information, request files, and log out. When we go to the request files where user details are available, there is an option that is normally a key in the action columns of the process called create key. When we click it, the key is delivered to the user's email address. The user validates the email, copies the OTP, and logs out of them.

4. To go to the user page means to go to the login page, then the user logins to the download file, and there is a download option available. Click it will ask for the OTP, then paste it view data, and it will show the file that we want them to download and open.

4.1 Algorithms

This paper provides 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.

Advanced Encryption Standard (AES) Algorithm

- The US chose the 2001 symmetric block cipher (Advanced Encryption Standard) to protect sensitive data.
- AES is a block cipher algorithm that can be used for encryption and decryption. AES contains three arrays: input, state, and key. The number of rounds depends on the key length, which spans from 128 bits to 12 rounds.
- The key size is 128/192/256 bits. The technique consists of 14 rounds, with a 256-bit key.

Step for AES Algorithm

- To initialize the state array, use the block data (plain text) and the starting state key, including the initial round key.
- Round keys should be derived from the encryption key.
- Complete the first nine rounds of state interference.
- During the eleventh and final round of state manipulation, copy the final state of encryption data (cipher text).

4.1.2 Elgamal Algorithm

- ElGamal algorithm is a public key cryptosystem that uses asymmetric key encryption. It deals with communication between two parties and encrypts their messages. The following cryptosystem, which employs primitive roots, was created in 1985. The system's security is determined by how difficult it is to solve the Problem with discrete logarithms r x a (mod p) or x = Indr(a). As demonstrated, appears to be essentially random as a function of a, making it a good choice for a basis of security.
- Every user of the ElGamal system: chooses and calculates a (large) prime p and one of its primitive roots r. The (secret) decryption key KD = k makes the encryption key KE = accessible, with 2 k p 2, 0 a p 1, and a = r k (mod p). Remember that in order to establish KD = k, an unauthorized person would have to do the extremely complex task of computing indr(a). To send a message to the user whose public key is KE =, the sender divides her message M into numerical blocks 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 might 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 hidden.
- Even though it is well known that KE = (p, r, a), calculating Indr is required to extract j from C1 (C1). However, the intended recipient computes B j without knowing whether or not they are aware that KD = k. The Fermat Theory is employed in the final 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 employing public key cryptography, encryption keys are not kept It is critical to be able to verify who sent each communication. [16] This article investigates the ElGamal public key encryption algorithm that is used in information transmission, indicating that it will reveal the numbers repeatedly performed on the data provider. Any member in an ElGamal cryptosystem can use their public and private keys to digitally sign any communication.

Using their own public key KE =, the message's sender derives the exponent j and computes c r j (mod p) (p,r, a). The sender then solves the linear congruence JD + kc B (mod p 1) for the first plaintext block B

by utilizing the EA.

- The sender's secret decryption key is KD = k. The sender then adds the digital signatures (c, d) to the encrypted messages. Keep in mind that in order to compute the secret variables k, j, and B, the sender must first obtain them. The recipient of the message utilizes 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). The signature is valid as long as V1 equals V2 (mod p).

5. Result Analysis

5.1 AES Algorithm Results:

Figure 11: File Upload Page in the cloud

In Fig 11, users enter a file name, parameter name, algorithms (AES or Elgmal), server name, server 2, and upload file (selected and uploaded).

Figure 12. File Upload Successfully in the cloud

In that case, we stored the information provided by the data providers in the cloud. It'll be saved to the cloud.

Figure 13. Upload files details

When the above fig. 13 is examined, it displays table columns such as serial number, filename, parameter name, server kinds, and cipher text of AESA algorithms that are present in the process.

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 such as 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 display the process's login page.

Figure 15. Search A File in the cloud

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

Figure 16. View Search File in the cloud

After clicking the search file, the preceding figure is displayed, indicating that the serial number, file owner name, file name, server name, view data status, and none represent the encryption text of the process's AESA algorithms.

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 implies that

when opened, it will display the above fig, which has been encrypted using the process's AES algorithms.

Figure 18. Request Send to the Cloud Provider

Figure 18 shows that we need to send the request to the cloud, then log out, visit the cloud provider, and accept the request in the cloud process.

Figure 19. View User Details in the cloud

Figure 19 shows that the cloud contains columns for user request files; to access the data, we must navigate to the columns: provider name, email ID, address registration date, status, accept or reject of the process, and so on.

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.

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.

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.

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.

Figure 24. View Users Requested Files Details in the cloud

Figure 24 shows the internal server with two columns: request file details and view server details, which are present because we needed to open request files. It will display the view user request file details in the following formats: data provider email id, user email id, and file name. The server name shows which server is uploading them, and the action indicates that it must generate a key for the process's user mail, so click it. It will generate a key.

Figure 25. Key in EMail id

In Figure 25, the internal server sends the key to the user's email address, which is then copied and used for the process's download file.

Figure 26. View Accepted Files for Downloading in the cloud

In fig. 26, after acquiring the key, go to the user login page and then to the process download file in the table column.

Figure 27. Download the File in the cloud

In Figure 27, pressing the "download file" button opens the enter key-value box labeled "download a file," and after copying the key in the box, we click the "view data" button to watch the process.

Figure 28. Output of AES Algorithm

6. Clicking on "view data" in the previous figure displays the output of the process's AES algorithms.

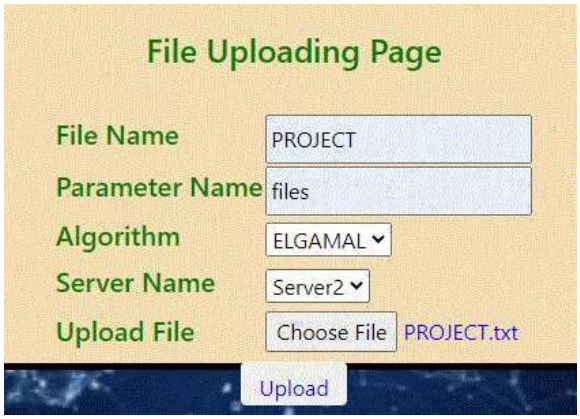

Figure 29: File Uploading Page in Elgamal in the Cloud

6.1. Elgamal Algorithm Results:

In fig. 29, users enter a file name, which is my file, a parameter name, which is the 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.

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.

Figure 31. Search File in the cloud

In the above figure 31. It is located on the user page and contains a table formatted with AEs and ELGAML encryption forms. In AEs, ciphertext will be in binary form, whereas in ELGAML, it will be in numerical form. I need to click the send request button, and the cloud provider will accept them. It will display accepted requests and information shared by the internal server before redirecting to the process's internal server.

Figure 32. View User Requested Files Details

In the above figure 32, The requested files will be displayed on an internal server page, with a table column including the data supplier email id, user email id, file name, file id, server name, and action. The key action will be executed, and the file will be opened. It creates a key and sends it to the user's email address.

Figure 33. Key in EMail id

In the above fig.33, the key has been sent by the internal server to the user's email address; copy the key and use it to download the process 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.

Figure 35. Download the File in the cloud

Figure 35 shows the "enter key value" box that displays after we copied the key from the box and clicked on "view data" for the procedure after clicking on the "download file" button.

Figure 36. Output of ElGamal Algorithms

7. After clicking on "view data" in the preceding figure 36, the output of the process ELGAMAL algorithms will be displayed.

7.1 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

8. Conclusion

To formalize the AES and ElGamal algorithms and secure the security of cloud data, I created a new searchable encryption scheme using our novel subset decision methods. I developed a distribution architectural approach and proved how the AES and ElGamal algorithms meet our specified security standards. In addition to the scheme, it has interesting features such as constant-size trapdoors, cipher text, and multi-keyword support. It also hides search and access patterns, and when searching, it allows for multiple writers and readers. The schemes are compared, and the findings reveal that our plan outperforms the others in terms of overall performance. I demonstrate how the HYBRID MODEL (AES and ElGamal) secures data via process-based interaction and computation between CP and IS.

References

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.
5. Practical 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/.
7. 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,

8. 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.
9. 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,
10. 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,
11. "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.
12. Q. Tang, Public Key Encryption Schemes Supporting the Equality Test with Different Granularity of Authorization, IJACT 2 (2012)
13. 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)
14. https://www.researchgate.net/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data
15. 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.
16. https://www.researchgate.net/publication/321348098_Cloud_Computing_A_Survey_on_ Service Providers
17. Bubak, M.; Kasztelnik, M.; Malawski, M.; Meizner, J.; Nowakowski, P.; Varma, S. International Symposium on Cluster, Cloud and Grid Computing (CC Grid) - Delft International Symposium on Cluster, Cloud, and Grid Computing - Evaluation of Cloud Providers for VPH Applications.
18. Fiat and M. Naor, "Broadcast encryption," in Annual International Cryptology Conference, 1993, pp. 480–491.
19. 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.
20. 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].