IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12510

DUAL - SERVER PUBLIC-KEY AUTHENTICATED ENCRYTION WITH KEYWORD SEARCH

Mr. M. NAGARASAN, M.E.[1], GAYATHRI.R[2], ALAGENDRAN.K[3], MARIMUTHU.P[4], PUSHPARAJ.S[5]

Assistant Professor- CSE, Info Institute of Engineering, Coimbatore[1]

(UG Scholars) Info Institute of Engineering, Coimbatore[2-5]

Abstract: In cloud storage, how to search sensitive data efficiently and securely is a challenging problem. The searchable encryption technique provides a secure storage method without loss of data confidentiality and usability. As an important branch of searchable encryption, public-key encryption with keyword search (PEKS) is widely studied by scholars. However, most of the traditional PEKS schemes are vulnerable to the inside keyword guessing attack (IKGA). Resisting the inside keyword guessing attack is likely to become an essential property of all new PEKS schemes. For a long time, mitigating IKGA has been inefficient and difficult, and most existing PEKS schemes fail in achieving their security goals. To address the above problems, we define the notion of Dual-server Public-key Authenticated Encryption with Keyword Search (DPAEKS), which protects against IKGA by leveraging two servers that do not cooperate, and supports the authentication property. Then, we provide a construction of DPAEKS without bilinear pairings. Experimental results obtained using a real-world dataset show that our scheme is highly efficient and provides strong security, making it suitable for deployment in practical applications.

Keywords: Cloud computing, security,DPAEKS adopts a dual-server framework, wherein the test functionality is split into two parts which are handled by two independent servers.

I. INTRODUCTION

The main aim is to is to provide secure and efficient searching of encrypted data in a cloud environment. It enables a user to delegate the storage of their data to cloud servers while still maintaining control over the confidentiality of the data.

It ensures that the data and the search queries are processed by two different servers. The user encrypts their data using a public key and uploads it to one server, while the search queries are sent to another server. This separation of data and search queries ensures that no single server has access to both the data and the search queries.The scope of DS-PKE-KWS is in the field of secure data storage and cloud computing, and it can be applied in various domains where sensitive data needs to be stored and protected while allowing authorized users to search for specific information without revealing any sensitive information to the cloud servers.

This is important in scenarios where sensitive data is stored in the cloud and needs to be protected from unauthorized access.

II. MATERIALS AND METHODS

- **SOFTWARE REQUIREMENTS**

➢	Operating system	:	Windows 11.
➢	Coding Language	:	JAVA.
➢	Tool	:	Apache Netbeans IDE 16
➢	Database	:	MYSQL
➢	Cloud	:	DriveHQ

- **HARDWARE REQUIREMENTS**

➢ System	:	Pentium i3 Processor
➢ Hard Disk	:	500 GB.
➢ Monitor	:	15’’ LED
➢ Input Devices	:	Keyboard, Mouse
➢ Ram	:	4 GB

User: The user is the entity that interacts with the system to search for specific information in the encrypted data. The user provides the search query and receives the encrypted search results.

Client: The client is the software or application that is installed on the user's device to enable the user to interact with the system. The client encrypts the search query and sends it to the servers.

Dual servers: The dual servers are the two servers that are responsible for storing the encrypted data and performing the search operation. The two servers work together to ensure that the search operation is secure and efficient.

Trapdoor function: The trapdoor function is a mathematical function that is used to generate a trapdoor from the search query. The trapdoor is used to identify the encrypted data that matches the search query, without revealing any information about the data or the query to the servers.

Encryption algorithm: The encryption algorithm is used to encrypt the data before it is stored on the servers. The encryption algorithm ensures that the data is secure and cannot be accessed by unauthorized users.

MODULES DESCRIPTION:

Data Owner (DO):

In this module we develop the Data Owner Module. This module represents the entity who owns the data and wants to store it securely on a cloud service. The DO is responsible for encrypting the data and sending it to the AS and the TS. The DO also generates the trapdoor for the DR to use when they want to access the data.

Data Receiver (DR):

In this module we develop the Data Receiver module. This module represents the entity who wants to access the encrypted data stored on the cloud service. The DR sends a trapdoor request to the system to retrieve the data. The DR does not have direct access to the encrypted data.

Assistant Server (AS):

In this module we develop the Assistant Server module. This module represents one of the two servers that store a copy of the encrypted data. The AS is responsible for generating intermediate cipher texts (ICTs) when the DR sends a trapdoor request. The AS receives the encrypted data from the DO and stores it securely. The AS also communicates with the TS to execute the test algorithm to check the validity of the ICTs. This module acts as an intermediary between the Data Receiver and the Test Server. It receives the search query from the Data Receiver, performs the necessary operations to generate the search token, and forwards it to the Test Server for further processing.

Test Server (TS):

In this module we develop the Test Server module. This module represents the second server that stores a copy of the encrypted data. The TS is responsible for testing the ICTs generated by the AS when the DR sends a trapdoor request. The TS receives the ICTs from the AS and executes the test algorithm to determine the validity of the request. The TS communicates the results of the test to the DR. This module represents the server that performs the actual keyword search operations on the encrypted data. It receives the search token from the Assistant Server, performs the keyword search using the DPAEKS scheme, and returns the search results to the Assistant Server, which then forwards them to the Data Receiver.

Intermediate Cipher Text (ICT):

This module represents the ciphertext generated by the AS in response to the trapdoor request from the DR. The ICT is sent to the TS for testing. The ICT does not reveal any information about the encrypted data stored on the cloud service. The system model provides a secure method for accessing encrypted files on cloud services. The use of two

DOI: 10.17148/IJARCCE.2023.12510

servers, each with a copy of the encrypted data, provides an additional layer of security to protect against data breaches. The ability to interchange the roles of the AS and the TS also improves the efficiency of the scheme in practical applications. This module represents the encrypted data stored in the cloud storage. The data is encrypted using the DPAEKS scheme, which provides strong security and ensures data confidentiality. The Intermediate Cipher Text is stored in the cloud storage and is used for keyword search operations without revealing the plaintext data to the cloud storage provider or any other unauthorized entities.

III. CONCLUSION

we have presented a new scheme called dual-server public-key authenticated encryption with keyword search (DPAEKS). The features of DPAEKS include: two non-colluding servers that are used to protect against IKGA and the data owner should be distributed with a pair of keys to authenticate the data. We developed a concrete construction of DPAEKS and proved its security. Finally, we implemented and evaluated the performance of the proposed scheme. The empirical results we obtained demonstrate that it is suitable for deployment in practical applications.

IV. DISCUSSION

DPAEKS has been proved to be secure, future work can involve further rigorous security analysis to identify and address any potential vulnerabilities or attack vectors. This can include formal security proofs, extensive testing, and evaluation against various types of attacks, including advanced attacks that may arise in real-world scenarios.

The performance evaluation of the proposed scheme may have demonstrated its suitability for practical applications, but future work can focus on further improving the scalability and efficiency of the scheme. This can involve optimizing the computational overhead, reducing communication overhead, and exploring techniques to handle larger keyword spaces or larger datasets to enhance the overall performance of the scheme in real-world scenarios

REFERENCES

[1] D. He, S. Zeadally, and L. Wu, “Certificateless public auditing scheme for cloud-assisted wireless body area networks,” IEEE Syst. J., vol. 12, no. 1, pp. 64–73, Mar. 2018.

[2] D. He, N. Kumar, M. K. Khan, L. Wang, and S. Jian, “Efficient privacy-aware authentication scheme for mobile cloud computing services,” IEEE Syst. J., vol. 12, no. 2, pp. 1621–1631, Jun. 2018.

[3] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, vol. 3027, pp. 506–522.

[5] P. Xu,H. Jin,Q.Wu, andW.Wang, “Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack,” IEEE Trans. Comput., vol. 62, no. 11, pp. 2266–2277, Nov. 2013.

[6] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “A new general framework for secure public key encryption with keyword search,” in Proc. Australasian Conf. Inf. Security Privacy, 2015, pp. 59–76.

[7] Q. Huang and H. Li, “An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks,” Inf. Sci., vol. 403, pp. 1–14, 2017.

[8] D. Wang, N. Wang, P. Wang, and S. Qing, “Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity,” Inf. Sci., vol. 321, pp. 162–178, 2015.

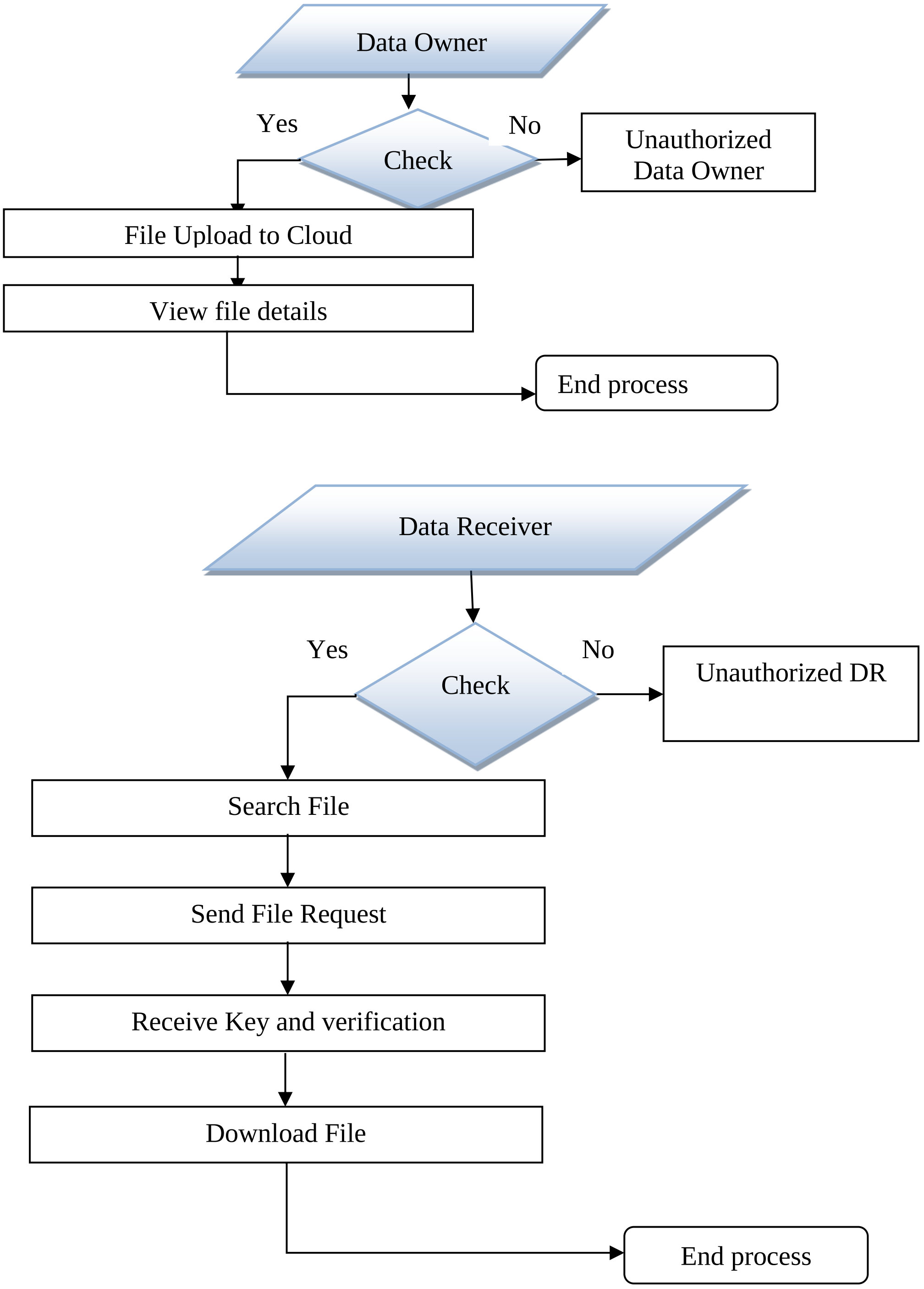
[9] D. He, Y. Zhang, D. Wang, and K. K. R. Choo, “Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography,” IEEE Trans. Dependable Secure Comput., 2018, doi: 10.1109/TDSC.2018.2857775.

[10] C.-h.Wang and T.-Y. Tu, “Keyword search encryption scheme resistant against keyword-guessing attack by the untrusted server,” J. Shanghai Jiaotong University (Sci.), vol. 19, no. 4, pp. 440–442, 2014.

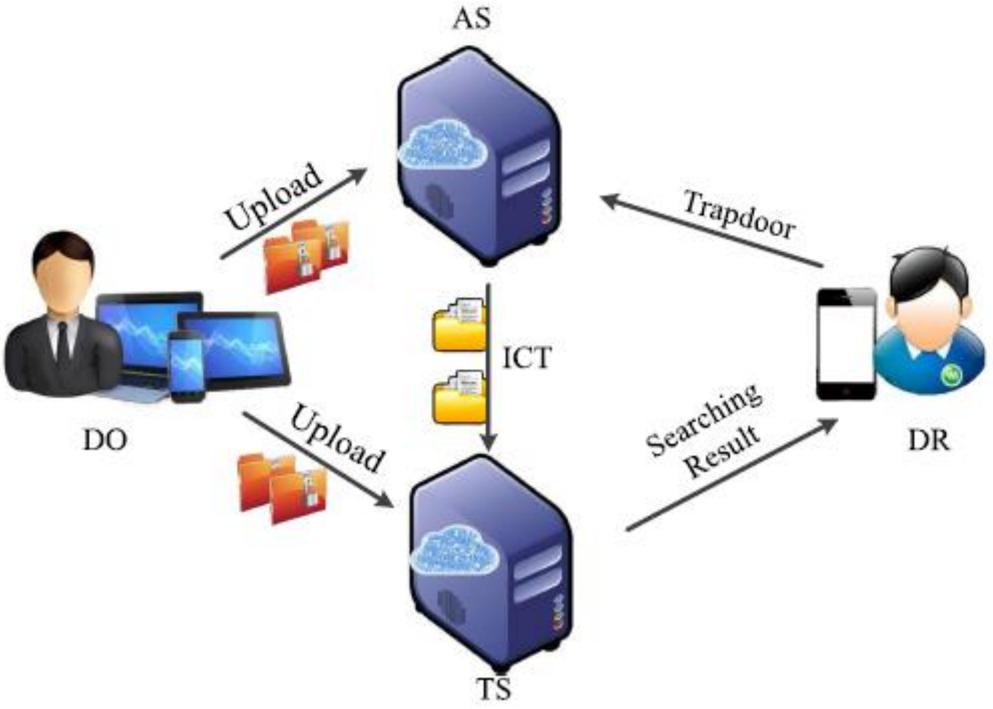
DOI: 10.17148/IJARCCE.2023.12510

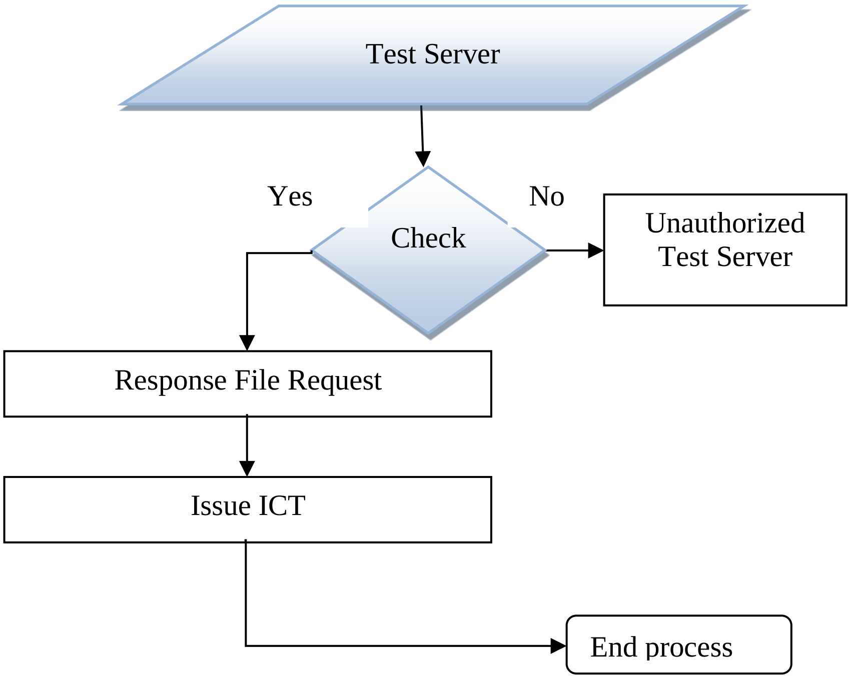
Data flow Diagram

Figure E.1: Flow Diagram Representation of the Project



DOI: 10.17148/IJARCCE.2023.12510


AS
Upload
Trapdoor
ICT
DO
DR
Upload
Searching Result
TS


Test Server
Yes
No
Check
Unauthorized Test Server
Response File Request
Issue ICT
End process