IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 7, July 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207163 |

Dual-Server Public-Key Authenticated Encryption and Search Retrieval

Kiran Kumar V[1], Prof. Sandarsh Gowda M M[2].

[1]MCA Graduate (2nd Year), Dept. of MCA, Bangalore Institute of Technology, Bangalore, Karnataka, India

[2]Asst.Professor, Dept. of MCA, Bangalore Institute of Technology, Bangalore, Karnataka, India

ABSTRACT: It is a difficult problem to rapidly and safely search sensitive data in cloud storage. The searchable encryption approach offers a safe way to save data without sacrificing its usefulness or confidentiality. Public-Key Encryption Keyword Search method for searching data on the cloud storage has received a set of attention from researchers. But it couldn't able to handle Inside Keyword Guessable Attack(IKGA) .On the other hand, the concerning notion of the "IKGA" can potentially undermine the core strengths of traditional PEKS methods.So all new PEKS schemes will likely need to have the ability to withstand the inside keyword guessing attack. IKGA mitigation has long proven ineffective and challenging, and the mainstream of current PEKS methods fall short of meeting their security objectives. We define the concept of Confidentiality with Dual Server Public Key Authenticated Encryption and Search Retrieval(DSPKAESR) which safeguards against IKGA by utilising two servers that do not communicate, and enables the authentication property, To be able to deal with the aforementioned issues. Next, we offer a DPIPL architecture without bilinear pairings. Our system is really effective and offers great security, according to experimental results obtained using a real-world dataset, making it appropriate for use in practical applications.

KEYWORDS: IKGA, DAS, DTS, ICT, DO, DR

I. INTRODUCTION

The mounting expansion of data in recent duration, cloud storage space has emerged as a potential paradigm .It not only provides consumers with on-demand storage, but it also provides obtaining information simpler on them. Data transferred to on-demand computers, on the other hand, might include private details (for example, business financial information or healthcare records), generating issues regarding privacy and security. Encrypting data before transferring it to a cloud-based server is a typical method of safeguarding data confidentiality. Nevertheless, encrypted information makes its usage more difficult, particularly the capacity to retrieve data.

The authors of Song et al. were the initial group to propose the notion of searchable encryption (SE), which depends on an asymmetric crypto-system and allows private information to be searched.

From that, Boneh et al. [4] created the notion of public-key cryptography with keyword searching (PEKS) and built a real approach to remove key administration and distribution based upon an uneven crypto-system.

The data proprietor, the data receiver (user), and the cloud server are all separate components in the PEKS framework. The records and keywords are encrypted by their information holder. The a cypher are subsequently sent to the internet server after being extracted from these documents with the information. beneficiary's public key. The data user submits an electronic mail to the remote server with the phrase that (s)he desires to search for. The server located in the cloud decides if the wording connected with the door and the term beneath the encryption text are the same. The cloud server returns the data that was encrypted matching to the backdoor.

II. LITERATURE SURVEY

S. Zeadally [1] proposed the utilization of circuits comprising multiple small, low-power sensors in WBANs, enabling real-time tracking of patients' physiology. This advancement holds the potential to significantly enhance patient monitoring and treatment for various illnesses. However, WBAN devices may have limitations in terms of computing, storage, power, and networking capabilities, which restrict the range of applications they can support. To address these limitations and bolster the capabilities of WBANs, the concept of cloud-assisted WBANs has been introduced. Cloud computing technology allows for state-assisted WBANs to offer more extensive features and handle patient medical data more effectively. In the case of online-assisted WBANs, patient physiology data resides in the cloud, and its integrity becomes of paramount importance as it is utilized for medical diagnoses and treatment planning.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207163 |

N. Kumar [2] highlights the increasing prevalence of handheld computers and the rapid expansion of data centers. To address the challenges posed by the limitations of storage, networking, and computation in handheld devices, the concept of mobile cloud processing (MCC) is proposed as a cutting-edge computing solution. MCC enables users to leverage cloud-based resources through their handheld devices, even while they are on the move. However, due to the inherent vulnerabilities in current wireless communication methods, ensuring privacy and security can be a challenging task.

In the context of security and privacy concerns, D.X. Song [3] suggests the use of encrypted data storage servers, such as mail servers and file servers, to mitigate risks. However, this approach often leads to a trade-off between security and functionality. Until recently, a significant challenge was how to enable data storage servers to perform searches and respond to queries without compromising the confidentiality of the data. For instance, a user might need to retrieve only documents containing a specific set of terms. The author presents cryptographic systems with security proofs, along with encryption solutions addressing the problem of searching encrypted data. These methods offer several important benefits in preserving both security and functionality.

In the research conducted by D. Bonesh [4], the focus is on searching encrypted data using a public key scheme. Consider a scenario where user Bob sends an encrypted email to user Alice, utilizing Alice's public key. The email gateway needs to check if the email contains the word "urgent" so that it can forward the communication accordingly. However, Alice is reluctant to grant the gateway access to all her message encryption keys. To address this concern, the study proposes a sophisticated method that enables Alice to provide the gateway with a specific key. This key allows the gateway to function and perform necessary actions without actually gaining full access to the details of the communication.

In the work of P. Xu and H. [5], they explore the concept of key-based security for keyword search, which proves to be a versatile technique. This approach allows a person, who possesses a method for a specific term, to search for encrypted content containing that keyword without being able to unlock the papers or learn the actual keyword itself. However, there is a vulnerability when the search term space is relatively large, where a malicious third party could potentially compromise the keyword through a brute-force guessing attack (KGA). To address this issue, the researchers propose a solution using encrypted public keys with a fuzzy query, introducing a variation of PEKS (Public Key Encryption with Keyword Search) that enhances keyword privacy. In this new method, each keyword is associated with both an exact and a fuzzy query trapdoor, and multiple keywords may share the same fuzzy query trapdoor, thereby mitigating the risks posed by the initial guess effort..

III. EXISTING MODEL

One common strategy is to encrypt the information before sending transfer it to a remote host safeguard its confidentiality. However, the encrypted data makes its use more challenging, especially the capacity for data retrieval.The malicious cloud server typically launches the IKGA, which has the potential to betray the privacy (such as identify or interests) of the receiver.

The IKGA is made possible by the malicious cloud server's ability to acquire the trapdoor, produce the ciphertext for any keyword, and repeatedly run the PEKS test method. Another factor is that practical apps typically do not have a large keyword space.

In order to locate the right keyword, the adversary can repeat the steps above. It is vitally necessary to develop security designs against the IKGA To simplify things easy use searchable encryption.

PEFKS (public-key encryption with furry keyword search was first proposed by Xu et al. Given that numerous keywords may use the same fuzzy trapdoor, the malicious server is unable to determine the precise keyword by using it.

Huang et al. also suggested a powerful PEKS against the IKGA. To prevent the malicious server inside from guessing the keyword in their scheme, the data owner is provided a key pair. However, the created trapdoor will remain the same if the keyword is left unchanged. This implies that the malicious cloud server would learn the keywords associated with the trapdoors and possess statistic knowledge of them.

- The fundamental reason why the current methods are vulnerable is that they lack the authentication attribute. This allows an adversary to develop a legitimate trapdoor keyword to search for encrypted data.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207163 |

- The computationally costly procedures needed because of the existing system techniques (such as map-to-point hashing and bilinear pairing) significant performance bottleneck in real-world applications.

IV. PROPOSED METHODOLOGY

The DPAESR model is used in the suggested system. The test functionality in DPAESR is separated into two components and is used by two separate servers under a dual-server system. No server can do independent testing. Assuming that the two servers are not working together, the security against the internal KGA is achieved.

The four entities in the wished-for system are, in order, the fact Data Owner(DO), Data Receiver (DR), Dual Authorization Server (DAS), and Dual Testopia Server (DTS). The DAS and TS receive the hidden data first from the DO. The DR can then send a trapdoor to query the saved data. As soon as DR sends request to access data, the DAS and TS authenticates and givess the secret key to DR so that he can use it to access encrypted data securely from cloud storage.

Advantages of Proposed System:

- The suggested approach can stop a rogue server from speculating IKGA based on the terms that a data user enters a query.
- The PEKS and Test algorithms in particular, and This suggested technique as a whole, have high computational efficiency. This is mostly because of the scheme's avoidance of operations that require a lot of computation. The dual-server architecture also makes our system immune to IKGA assaults. It needs to be noted that since the test requires contact with both servers, resisting IKGA is only possible at the penalty of communication overhead.

IMPLEMENTATIONS

1) Data Owner

This module represents the entity that owns the statistics and wishes to safely store it on theinternet. The responsibility of encrypting data and transmitting it to the DAS (Authorization Server) and DTS (Testopia Server) lies with the DO (Data Owner). Additionally, the DO is responsible for generating the trapdoor that the DR (Data Requestor) can use to access the encrypted data.

2) Data Receiver

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 do not have shortest right to use to the encrypted data.

3) Dual Authorization Server

This particular component of the system is one of the two computers that hold a copy of the encrypted data. When the DR submits a loophole request, the DAS (Authorization Server) takes charge of creating Initial Cypher Tokens (ICT). The DAS receives encrypted information through the DO (Data Owner) and securely stores it. Moreover, the DAS collaborates with the DTS (Testopia Server) to execute the testing process and validate the ICT. This module serves as an intermediary between the Data Receiver and the Testopia Server. It receives the search query generated by the Data Receiver, generates the token, and sends it to the DTS for further processing.

4) Dual Testopia Server

The Testopia Server module is created in this module. This module represents the second server, which holds an encrypted duplicate of the data. When the DR submits a trapdoor request, the DTS is in charge of checking the ICT created by the DAS. The DTS gets the ICT from the DAS and lope the check algorithm to assess the request's legitimacy. The test findings are communicated to the DR by the DTS.This module represents the server that actually does keyword searches on the encrypted material. It gets the search token from the Authorization Server, does the keyword search using the DSPKAESR scheme.

Intermediate Cypher Token

This module contains the cyphertext created by the DAS in response to the DR's trapdoor request. The ICT is forwarded to the DTS for testing. The ICT provides no details on the encrypted data kept on the cloud service.The

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207163 |

system concept provides a safe way to access encrypted information stored on cloud services. The usage of two servers, each with a copy of the encrypted data, adds an extra degree of protection against data intrusions. The flexibility to switch between DAS and DTS responsibilities increases the scheme's efficiency in actual situations.This module represents the encrypted data that is saved on the cloud. The data is encrypted with the DPAESR technique, which guarantees high security and privacy.

V. CONCLUSION

This paper presents a novel conduct called dual server public key identification and phrase lookup (DSPKAESR). Within the characteristics of DSPKAESR are two non-colluding servers that are used to avoid IKGA. Furthermore, the info holder ought to have provided with a set of keys to authenticate the data. We built a steel DSPKAESR structure and showed its safety. Lastly, we implemented the proposed system and tested its efficacy. Our tests show that it is suitable for usage in real-world scenarios**.**

REFERENCES

[1] D. He, S. Zeadally, and L. Wuu, "Certificateless public auditingscheme for cloud-assisted wireless body area networks," IEEE Systems Journal, vol. 12, no. 1, pp. 64-73, Mar. 2018.
[2] D. He, N. Kumar, M. K. Khan, L. Wang, and S. Jian, "Efficientprivacy-aware authentication scheme for mobile cloud computingservices," IEEE Syst. J., vol. 12, no. 2, pp. 1621-1631, June 2018.
[3] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques forsearches on encrypted data," in Proc. IEEE Symp. Security Privacy, 2000, pp. 44-55.
[4] D. Boneh, G. Di.. Crescenzo, R. Ostrovsky, and G. Persiano, "Publickey encryption with keyword search," in Proceedings of the International Conference on Theory and Applications of Cryptographic Technology, 2004, vol. 3027, pp. 506-522.
[5] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzykeyword search: A provably secure scheme undZr keyword guessing attack," IEEE Trans. Comput., vol. 62, no. 11, Nov. 2013, pp. 2266-2277.
[6] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "A new generalframework for secure public key encryption with keyword search," Australasian Conf. Inf. Security Privacy, 2015, pp. 59-76.
[7] Q. Huang and H. Li, "An efficient public-key searchable encryptionscheme secure against inside keyword guessing attacks," Inf.Sci., vol. 403, pp. 1-14, 2017.
[8] D. Wang, N. Wang, P. Wang, and S. Qing, "Freeing up privacy: An efficient and provably secure two-factor authentication scheme with user annonymity," Inf. Sci., vol. 321, pp. 162-178, 2015.
[9] D. He, Y. Zhang, D. Wang, and K. K. R. Choo, "A 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 to keyword-guessing attack by an untrusted server," Journal of Shanghai Jiaotong University (Sci.), vol. 19, no. 4, pp. 440-442, 2014.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details