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.2023.1207192 |

Future Safe Public Key Encrypted for Outsourced Cloud Storage Using Topical Look

Rahul N Swamy[1], N Rajeshwari[2]

Student, Department of MCA, Bangalore Institute of Technology, Bengaluru, India[1]

Assistant Professor, Department of MCA, Bangalore Institute of Technology, Bengaluru, India[2]

ABSTRACT: The greatest tool now for limiting data leak is secrecy, and cloud storage has emerged as a key sector in distant data management services. One of these, the use of public keys with search terms (PKSE), is seen as a promising method since it enables visitors to search fast through encrypted data files. In other words, when a client wants to scan data files, the client first produces a search coin, which the cloud server then utilises to continue the inquiry across encrypted data files. However, when PKSE and cloud combine, a major attack is posed. Formally speaking, the online server may use the search flags it got to learn the details of a new secure file containing a term that was previously asked and can also learn the privacy details. We suggest a forward safe public key indexing strategy to overcome this problem, in which an online server can't suss out anything a recently uploaded secured file having the keyword that was previously queried. We offer a framework for creating forward safe public key searchable codes based on attribute-based visible encrypt in order to better grasp the design approach. Finally, the experiments prove the value of our plan.

KEYWORDS: Cloud, Keyword, Encryption, Token,PKSE

I. INTRODUCTION

Cloud computing is the usage of software and hardware for PCs that is provided as an option across a network, most often via the web. The term arises from a common use of a cloud-shaped sign in system diagrams as a metaphor for the intricate architecture it holds. The use of clouds entrusts the data, software, and processing of a user to remote services. Software and physical The makes materials available via web via regulated third-party services in cloud computing. These services often give users access to cutting-edge server networks and complex software tools.

The cloud's use aims to apply conventional supercomputing, or powerful processing power typically used by military scientific facilities, to run tens of trillions of operations per second in consumer-oriented applications like financial portfolios, deliver personalised details, provide data storage, or power greatly multi-player online games.

Nets of massive clusters of computers, frequently utilising low-cost client PCs with specialised connections, are employed in clouds computing environment to spread data processing tasks among them. Large networks of interconnected systems make up this common IT infrastructure. The power of the cloud is frequently maximised through the usage of virtualization methods. Due to the Institute of Devices and Terminology's (NIST) definitions, the key aspects of the cloud are as follows:

- **On-demand self-service:** A customer may instantly supply IT assets as needed, such as cpu time and network drives, without needing to deal with the supplier of each service in person.

- **Wide-ranging web access:** Skills are made visible over the web and access via common mechanisms to encourage use by various thin- or thick-client platforms (such as mobile phones, computers, and PDAs).

|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 ||

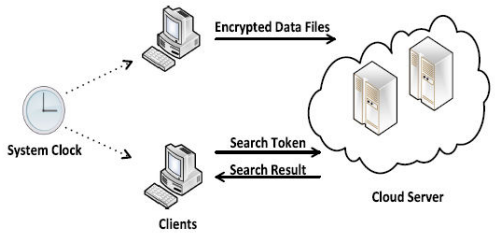
| DOI:10.15680/IJIRSET.2023.1207192 |

Resource pooling: Using a multi-tenant structure, the provider's computing resources are combined to serve many users, with different kinds of resources being dynamically allocated and moved in response to customer demand. The client typically has no say or influence over the precise location of the resources given, but they might be able to designate location at another level of generality (for example, nation, state, or data centre). This gives the consumer a perception of geographical independence. Storage, computation, memory, internet traffic, and virtual machines are a few examples of supplies.

II. LITERATURE SURVEY

It is now emerging as a new concept for obtaining hidden data from large data. Big data collecting and use generate substantial privacy problems in addition to producing significant values. A simple solution to safeguard the vast volume of perhaps private info is to encrypt it using specialised cryptography tools. However, using or working with encrypted data might be difficult, in particular when utilising AI methods. The challenge of training high-quality word vectors over vast quantities of encrypted data (from remote data owners) using collective network learning techniques is examined in this paper. We use data encrypted as part of our build and also develop a set of arithmetic primitives (such as adding, fixed-point voting, sigmoid function computation, etc.). We undertake thorough tests on typical real-world datasets to confirm the viability and efficacy of our suggested form and logically analyse its efficacy and safety.

Based on cutting-edge cellular and networking technology, car [2] ad-hoc networks (VANETs) have been built. For VANET security, message credentials between cars and roadside units are crucial. If they could be knew, messages needed to be signed and authenticated. Vehicles' true identities should not be made public and should only be tracked by authorised parties. Present offerings either cannot meet the security requirement or largely rely on tamper-proof hardware. Another problem, communication overhead, is also not well addressed in prior research which was published. In this study, we suggest the SPACF scheme, a software-based solution devoid of any specialised hardware, to overcome such issues. The Cuckoo Sort and binary search strategies use. Existential unforgeability of the underlying sign against adapted chosen-message attack can be seen with the Elliptic Curve Di A logarithm Issues in the random oracle model to ensure that it can meet the message authentication criterion. Because it is pairing-free and doesn't employ map-to-point hash functions, the The results indicate our proposed approach is more efficient than earlier schemes and meets the security and privacy criteria of vehicular network ad hoc.



Fig[1] System Architecture

III. EXISTING SYSTEM

By introducing the idea of public key searches encoding, Boneh et al. shown that it outperforms symmetric searchable keys when sharing data.

He et al. propose an overall system to demonstrate how faceless encryption using identity may be converted to public key lookup crypto.

|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.2023.1207192 |

Khader et al. propose a method using kresilient identity-based encoding, which can be shown to be safe in the standard model but must assume the amount of illicit clients is less than a certain value, to avoid utilising random oracles.
By giving the server its public and secret key tandem, Baek et al. are able to get around the limit of utilising a secure channel. Emura et al. then expand this method to defend against flexibly enemies.

IV. PROPOSED SYSTEM

In this study, we offer fresh, strong forward-secure key public security technique. We find a non-trivial fix to the first two engineering issues in order to develop the system. The plan states that a cloud server won't be able to tell if a query token fits a secure data file if it does a search action of the two even though the former was produced before the latter. Additionally, we given exact structure for obtaining forward-secure public key lookup locks such that the basic design idea may be easily realised.

> The model of security makes the assumption that clients are sincere and will follow protocols in an honest manner. The digital clock is a completely reliable source that will always accurately inform customers of the energy. The haze servers, to honestly store secured data files and run the suggested protocols, is also believed to be inquisitive about the material of data files and queries. As a result, the cloud server tries to deduce the secret details of searches and data files. The security under the premise prevents the cloud host from picking up any skills other than the test results during the search phase.

Our instinct tells us to connect a search token's (or an encrypted data file's) creation time to the token's generation time in order to accomplish advance privacy for public key reusable encryption. The system initially determines if the private information file was produced prior to the search token before beginning to execute the search.

V. IMPLEMENTATION

MODULES:

Clients:

This module represents the end-users of the system who want to search for records in the air server. The Clients module interacts Using a cloud host module to submit search queries and retrieve the search results. It also interacts with the System Clock module to ensure that the search tokens generated by the clients are valid.
In this module, The entity needs to get records from a cloud server in addition to storing significant amounts of data files on the cloud server.
A client creates a search engine token using the querying term and transmits a To find data files on the cloud server, send a search token. The internet server may search encrypted files after obtaining a search token in order yield results.

Cloud Server:

In this part we develop the Cloud Module. The Cloud Server module is responsible for securely storing the encrypted cloud files containing the user's data and performs the search operations.
The group, which has abundant storage and processing capacity, offers its customers services in the cloud.

|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.2023.1207192 |

With online storage, a client gets to upload their data files to a server in the cloud in order to free themselves from number of managerial tasks or to collaborate on data files with others using a server in the cloud. A record of data should be classified before uploading in order to protect private.

In We need for public key visible key frauds to share their information files with forward security, preventing a search token from being used to find for concealed data files that were produced after the time y at which it was formed (for instance, a search token written at time t cannot be utilised to locate a secret record made at time period). y). t0, where t1 > t).

This module represents the centralized server that stores the encrypted data files and performs the search operations. The Cloud Server module receives search queries from the Clients module, executes the search process, and gives the corresponding results to the clients. It also interacts with The System Timer module to make sure the search tokens are exact submitted by the clients are valid.

DriveHQ is a hosting company that we employ for cloud storage, and the data provided by the user will be held in the DriveHQ cloud service.

System Clock:

The entity is responsible for the global time of the system, it tells clients the current time period.

This module represents the trusted entity in the system that maintains the current time. The System Clock module provides the current time to the Clients and Cloud Server modules, which ensures that the search tokens generated by the clients and the encrypted data files stored by the server are valid. The System Clock module also ensures the forward security of the system by binding the search tokens and the generation time of the encrypted data files.

VI. CONCLUSION

In this paper, we study the forward security for public keysearchable encryption, which means a new addedencrypted data file cannot be searched by the search tokensgenerated before the encrypted data file. This security isurgently required for the Private data that leaks to a cloud server can be greatly reduced by public key lookup encrypted methods used in cloud storage. Then, by establishing a general framework, we demonstrate how to create a forward safe publickey searchable encryption strategy from an attribute-based search encryption strategy. This concrete system is based on the 0-Encoding and 1-Encoding approach. In order to demonstrate the viability of our suggested approach In respect to search, token era, and encoding, we design tests.

REFERENCES

[1] Q. Wang, M. Du, X. Chen, Y. Chen, P. Zhou, X. Chen, andX. Huang, “Privacy-preserving collaborative model learning: Thecase of word vector training,” IEEE Trans. Knowl. Data Eng.,vol. 30, no. 12, pp. 2381–2393, Dec. 2018.
[2] J. Cui, J. Zhang, H. Zhong, and Y. Xu, “SPACF: A secure privacypreservingauthentication scheme for VANET with cuckoo filter,”IEEE Trans. Veh. Technol., vol. 66, no. 11, pp. 10283–10295,Nov. 2017.
[3] H. Zhong, W. Zhu, Y. Xu, and J. Cui, “Multi-authority attributebasedencryption access control scheme with policy hidden forcloud storage,” Soft Comput., vol. 22, no. 1, pp. 243–251, 2018.
[4] D. X. Song, D. A. Wagner, and A. Perrig, “Practical techniques forsearches on encrypted data,” in Proc. IEEE Symp. Security Privacy,2000, pp. 44–55.
[5] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky,“Searchable symmetric encryption: Improved definitions and efficientconstructions,” in Proc. ACM Conf. Comput. Commun. Security,2006, pp. 79–88.
[6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Publickey encryption with keyword search,” in Proc. Int. Conf. TheoryAppl. Cryptographic Techn., 2004, pp. 506–522.

|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.2023.1207192 |

[7] Y. Zhang, J. Katz, and C. Papamanthou, "All your queries arebelong to us: The power of file-injection attacks on searchableencryption," in Proc. USENIX Security Symp., 2016, pp. 707–720.
[8] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,J. Malone-Lee , G. Neven, P. Paillier, and H. Shi, "Searchableencryption revisited: Consistency properties, relation to anonymousIBE, and extensions," in Proc. Annu. Int. Cryptology Conf.,2005, pp. 205–222.
[9] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order-preservingencryption for numeric data," in Proc. ACM Conf. Manage. Data,2004, pp. 563–574.
[10] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-preservingsymmetric encryption," in Proc. Int. Conf. Theory Appl.Cryptographic Techn., 2009, pp. 224–241.

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