PRIVACY-PRESERVING AND TRUSTED KEYWORD SEARCH FOR MULTI-TENANCY CLOUD

SHAGAM GEETHA[1], POLISHETTY VENNELA[2], GORIGE SRUTHI[3], ALAKUNTLA LAXMI NARASIMHA[4], MALLELA PAVAN SAI[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Cloud service models intrinsically cater to multiple tenants. In current multi-tenancy model, cloud service providers isolate data within a single tenant boundary with no or minimum cross-tenant interaction. With the booming of cloud applications, allowing a user to search across tenants is crucial to utilize stored data more effectively. However, conducting such a search operation is inherently risky, primarily due to privacy concerns. Moreover, existing schemes typically focus on a single tenant and are not well suited to extend support to a multi-tenancy cloud, where each tenant operates independently. In this article, to address the above issue, we provide a privacy preserving, verifiable, accountable, and parallelizable solution for "privacy-preserving keyword search problem" among multiple independent data owners. We consider a scenario in which each tenant is a data owner and a user's goal is to efficiently search for granted documents that contain the target keyword among all the data owners. We first propose a verifiable yet accountable keyword searchable encryption (VAKSE) scheme through symmetric bilinear mapping. For verifiability, a message authentication code (MAC) is computed for each associated piece of data. To maintain a consistent size of MAC, the computed MACs undergo an exclusive OR operation. For accountability, we propose a keyword based accountable token mechanism where the client's identity is seamlessly embedded without compromising privacy. Furthermore, we introduce the parallel VAKSE scheme, in which the inverted index is partitioned into small segments and all of them can be processed synchronously. We also conduct formal security analysis and comprehensive experiments to demonstrate the data privacy

preservation and efficiency of the proposed schemes, respectively.

Index Terms – Cloud computing, multi-tenancy, searchable encryption, privacy-preserving keyword search, verifiable searchable encryption, accountable searchable encryption, symmetric bilinear mapping, message authentication code (MAC), parallel keyword search, inverted index, cloud security, data privacy, access control.

I. INTRODUCTION

Cloud computing provides large-scale storage, computing power, and flexible services, making it popular for applications like healthcare. In multi-tenancy cloud environments, different organizations (tenants) store their data on the same cloud platform.

For example, patient records and doctor information may be stored by different healthcare providers. Searching across these encrypted datasets is difficult because each organization must protect user privacy and comply with regulations like HIPAA. To ensure confidentiality, data owners encrypt their data before uploading it to the cloud. However, encryption makes searching inefficient because users would otherwise need to download and decrypt all data. Searchable Symmetric Encryption (SSE) solves this problem by allowing keyword searches over encrypted data without decryption. Later research improved SSE by introducing secure indexes, stronger security models, and verification mechanisms to ensure search correctness and completeness. However, these solutions often require high storage and computation costs. Fine-grained access control using Attribute-Based Encryption (ABE) was also introduced to allow only authorized users to search encrypted data.

Despite these improvements, existing methods mainly support searching data owned by a single organization. In real-world scenarios, users such as doctors often need to search encrypted data from multiple independent data owners. Current approaches either generate many separate search requests or require expensive multi-writer database systems.

Therefore, there is a need for a privacy-preserving, efficient, and trusted keyword search scheme that supports secure searching across multiple tenants in cloud environments while maintaining data privacy and reducing computational overhead.

II. RELATED WORK

A. *Attribute-based expressive and ranked keyword search over encrypted documents in cloud computing*

In recent years, several new notions of security have begun receiving consideration for public-key cryptosystems, beyond the standard of security against adaptive chosen ciphertext attack (CCA2). Among these are security against randomness reset attacks, in which the randomness used in encryption is forcibly set to some previous value, and against constant secret-key leakage attacks, wherein the constant factor of a secret key's bits is leaked. In terms of formal security definitions, cast as attack games between a challenger and an adversary, a joint combination of these attacks means that the adversary has access to additional encryption queries under a randomness of his own choosing along with secret-key leakage queries. This implies that both the encryption and decryption processes of a cryptosystem are being tampered under this security notion. In this paper, we attempt to address this problem of a joint combination of randomness and secret-key leakage attacks through two cryptosystems that incorporate hash proof system and randomness extractor primitives. The first cryptosystem relies on the random oracle model and is secure against a class of adversaries, called non-reversing adversaries. We remove the random oracle oracle assumption and the non-reversing adversary requirement in our second cryptosystem, which is a standard model that relies on a proposed primitive called lossy functions. These functions allow up to M lossy branches in the collection to substantially lose information, allowing the cryptosystem to use this loss of information for several encryption and challenge queries. For each cryptosystem, we present detailed security proofs using the game-hopping procedure. In addition, we present a concrete instantiation of lossy functions in the end of the paper—which relies on the DDH assumption.

B. *Secure keyword search and data sharing mechanism for cloud computing*

The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to

conduct a quick search and return the result without losing data confidentiality. To overcome these problems, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword in our scheme can be updated during the sharing phase without interacting with the PKG. In this article, we describe the notion of CPAB KSDS as well as its security model. Besides, we propose a concrete scheme and prove that it is against chosen ciphertext attack and chosen keyword attack secure in the random oracle model.

C. Omnes pro uno: Practical multi-writer encrypted database

Multi-writer encrypted databases allow a reader to search over data contributed by multiple writers securely. Public-key searchable encryption (PKSE) appears to be the right primitive. However, its search latency is not welcomed in practice for having public key operations linear in the entire database.

In contrast, symmetric searchable encryption (SSE) realizes sublinear search, but it is inherently not multi-writer. This paper aims for the best of both SSE and PKSE, i.e., sublinear search and multiple writers, by formalizing hybrid searchable encryption (HSE), with some seemingly conflicting yet desirable features, requiring new insights to achieve.

Our first contribution is a history-based security definition with new flavors of leakage concerning updates and writer corruptions, which are absent in the only known multi writer notion of PKSE since it is vacuously secure against writers. HSE, built on top of dynamic SSE (DSSE), should satisfy the de facto standard of forward privacy. Its multi writer support, again, makes the known approach (of secret state maintenance) fails. HSE should also feature efficient controllable search – each search can be confined to a different writer subset, while the search token size remains constant. For these, we devise a new partial rebuild technique and two new building blocks (of independent interests) – ID-coupling key-aggregate encryption and (optimal) epoch-based forward-private DSSE. Our evaluation over real-world datasets shows that HSE, surpassing prior arts by orders of magnitude,

is concretely efficient for popular multi-writer database applications.

D. A general transformation from KP ABE to searchable encryption

Users are inclined to share sensitive data in a remote server if no strong security mechanism is in place. Searchable encryption satisfies the need of users to execute a search encrypted data. Previous searchable encryption methods such as “public key encryption with keyword search (PEKS)” restricted the data access to certain users, because only the assigned users were able to search the encrypted data. In this paper we will discuss the relation between Attribute Based Encryption (ABE) and searchable encryption and define a weak anonymity of the ABE scheme, named “attribute privacy”. With this weak anonymity, we propose a general transformation from ABE to Attribute Based Encryption with Keyword Search (ABEKS) and a concrete attribute private key policy ABE (KP-ABE) scheme. We present an ABEKS scheme based on this KP-ABE scheme and permit multi-users to execute a flexible search on the remote encrypted data.

III. PROPOSED METHODOLOGY

The multi-tenant cloud framework is a specialized architecture that transforms how secure data operations are designed by addressing the common problem of administrative isolation and single-tenant scaling limitations. Traditional cloud search networks often struggle with this issue, where the query protocols and indexing structures diminish in efficiency as they pass through multiple independent data domains, making it hard for the model to securely and uniformly execute parallel operations across isolated environments. Developed to overcome these performance constraints, this framework introduces a novel approach known as "cross-owner indexing," which allows search criteria to flow directly across disparate data silos through privacy-preserving shortcut links. These indexing links securely bypass structural isolation boundaries, effectively enabling the search protocol to "skip" individual decryption pipelines and directly connect a user's query token to an independent data owner's encrypted output. This mechanism maps the search tokens from the user to the corresponding ciphertexts of deeper layers, which simplifies the task for the Cloud Service Provider (CSP) by letting it evaluate matching keywords, or data residuals, between the query and the secure indices rather than forcing it to decrypt or learn entire datasets from scratch. This structure of

"independent cryptographic blocks" enables the framework to scale across hundreds or even thousands of data owners without encountering the privacy leak or bottleneck problems that often affect traditional centralized cloud architectures. One of the most notable achievements of this multi-owner framework is its impact on secure data processing, a highly competitive benchmark area for cloud computing efficiency. The framework achieves state-of-the-art results in multi tenant data retrieval, reducing search latency significantly while setting new standards for verifiable accountability and parallel execution. Moreover, this parallelizable search approach has found applications in other fields, including distributed ledger technology (blockchain) and secure multi-party computation (SMPC).

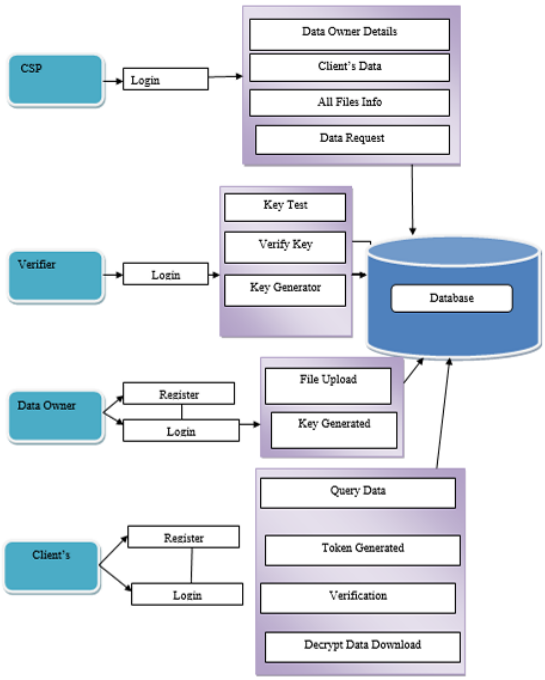


Fig. 1: System Overview

1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2. CSP

This is the first module the cloud services has a login with a mail id and password. The CSP has a data owner details. The CSP has a generated a key. The CSP has a client's details. The CSP have a requested a data. The CSP has a stored a file details. The CSP has a clients add all the members.

3. Verifier

This is the Second module of this project the Verifier has a login with a mail id and password. A verifier has a key has a key test it is generated original key or duplicate key. It also have a verify a key then it will send to the data receiver. The verifier has a verification key matching to the data.

4. Data Owner

This is the third module of this project. In this project data holder has a register with all details and login with a user id and password. The data owner has a file upload to store a data. The data owner has a key generated to share a data.

5. Clients

This is the fourth module of this project. Clients has a register with all details and then login with a email id and password. The client's has a query data. The client has a token generated to a private key. The client has a verification a data. The Client has a decrypt a data.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed VAKSE framework enables privacy-preserving, verifiable, and accountable keyword search across multiple cloud tenants with high efficiency. The use of MAC-based verification, keyword-based accountable tokens, and parallel inverted index processing reduces search time while ensuring data integrity and user accountability. Security analysis confirms strong privacy protection without compromising search accuracy. Overall, the proposed scheme provides a scalable and efficient solution for secure keyword search in multi-tenancy cloud environments.



Fig. 2: Home Page

International Journal of Engineering Research and Science & Technology

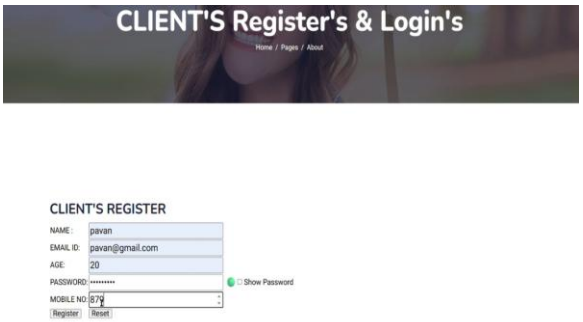


Fig. 3: Clients Registration

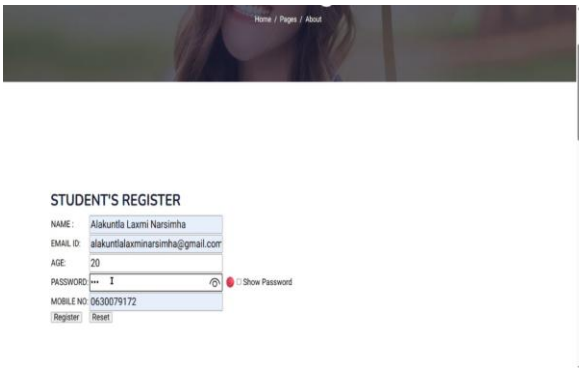


Fig. 4: Student Register

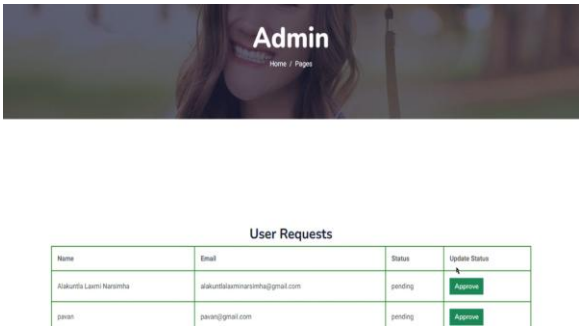


Fig. 5: User Requests

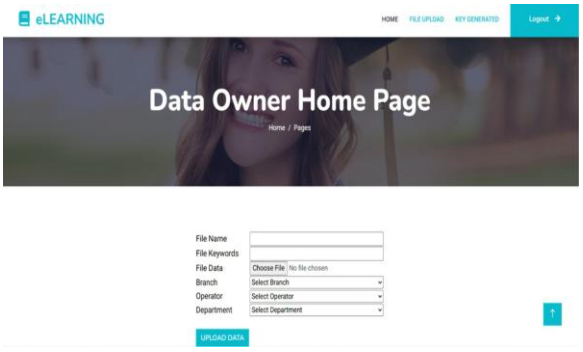


Fig. 6: Upload Data

V. CONCLUSION

Herein, we propose a privacy-preserving, efficient, verifiable, accountable, and parallel solution for the keyword search problem in a multitenant cloud environment. To achieve this, we devised a privacy-preserving inverted index to enable a verifiable ciphertext search. Each entry contains encrypted keyword and document identity pairs and the compressed MAC for all corresponding documents. Then, we designed a fine-grained access control mechanism through keyword-based token generation. Moreover, we embedded the user identity into the token to achieve user accountability. All those components were built into the VAKSE scheme. To further improve search efficiency, we introduced the PVAKSE, in which the inverted index was partitioned into small segments that could be searched synchronously.

REFERENCES

[1] (2022). Healthvana. [Online]. Available: https://healthvana.com

[2] (2022). CDPHP. [Online]. Available: https://www.cdphp.com

[3] (2022). Customer Success Stories. [Online]. Available: https://aws.amazon.com/solutions/case-studies/

[4] (2022). HiPAA. [Online]. Available: http://www.cms.hhs.gov/ HIPAAGenInfo

[5] D. Xiaoding Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy. (S&P), May 2000, pp. 44–55.

[6] E.-J. Goh, "Secure indexes," Cryptol. ePrint Arch., Oct. 2003.

[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," J. Comput. Secur., vol. 19, no. 5, pp. 895–934, 2011.

[8] Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest but-curious cloud servers," in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2012, pp. 917 922.

[9] C. Chen et al., "An efficient privacy-preserving ranked keyword search method," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 4, pp. 951–963, Apr. 2016.

[10] F. Han, J. Qin, H. Zhao, and J. Hu, "A general transformation from KP ABE to searchable encryption," Future Gener. Comput. Syst., vol. 30, pp. 107–115, Jan. 2014.

AUTHORS Profile



Mrs. SHAGAM GEETHA has received her B.Tech in 2012 from Nagarjuna Institute of Technology, JNTUH. She completed her M.Tech in Computer Science and Engineering (CSE) in 2014 from Vidya Vikas Institute of Technology, JNTUH.



Ms. POLISHETTY VENNELA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. GORIGE SRUTHI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. ALAKUNTLA LAXMI NARASIMHA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. MALLELA PAVAN SAI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.