IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

Multi Tenancy Cloud Data with a Shared Privacy Preserving Trusted Keyword Search

Mr. G. Lakpathi[*1], Saurav Kumar Mandal[*2], Deekshita Thumma[*3], Heerakar Abhishek[*4]
[*1]Associate Professor, Department of Computer Science & Engineering
[2,3,4]Students, Department of Computer Science & Engineering
Guru Nanak Institute of Technology, Ibrahimpatnam, Telangana, India

Abstract: *In 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*

Keywords: Cloud Service, Database, Cloud Service Providers, Privacy Preserving, Message Authentication Code (MAC), Multi-tenancy cloud

I. INTRODUCTION

CLOUD computing has had a profound impact on data management. It offers massive storage and computing resources, payment-on-demand, and flexible scalability. Motivated by these advantages, thousands of clients are opting for cloud services. One typical application area is healthcare, and some applications are Healthvana [1] and CDPHP [2]; both the platforms are the tenants of Amazon [3]. Healthvana stores patient reports and CDPHP stores doctor information. It is desirable for a patient to search both the datasets to find the most suitable doctor by matching the patient data with the doctor information. For example, HIV patients store their reports in Healthvana and seek for suitable doctors from CDPHP. However, such a search across tenancies is challenging. Each tenant is an independent data owner and must abide the privacy laws, such as HIPAA [4], which are enforced to protect individuals' medical data privacy. In addition, for their own interests, companies treat patient data as an asset and tend to maintain complete control over it. Data encryption is the best practice for maintaining data privacy. Each data owner encrypts their data before outsourcing it to the cloud. This guarantees the confidentiality of the data but greatly reduces their utility. A user must download an entire dataset in order to retrieve one piece of data. Considering data utility and privacy, Song et al. [5] introduced the primitives of symmetric searchable encryption (SSE). SSE is a keyword search technique that allows search over the cipher text without decryption. Goh et al. [6] proposed a secure index to improve search efficiency. Subsequently, Curtmola et al. [7] formalized the security definition of SSE and proposed two constructions that corresponded to non adaptive semantic security and adaptive semantic security. In early research, most works on SSE focused on the honestbut-curious cloud service provider (CSP). In such a model, the search result is fully trusted and the CSP is assumed to honestly follow the protocol specification. Search results in practice may contain corrupted data due to underlying hardware/software failures. In addition, for self-interest, the CSP may deviate from the protocol

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

specification. For example, to reduce computational costs, CSP may randomly choose data as a search result. To mitigate this problem, Chai and Gong [8] proposed verifiable SSE, where the search result includes not only retrieved documents but also proof of the correctness and completeness of the search.

II. LITERATURE SURVEY

[1]**TITLE**: Attribute-based expressive and ranked keyword search over encrypted documents in cloud computing
AUTHOR: Q. Huang, G. Yan, and Q. Wei
YEAR: 2023
DESCRIPTION: 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.
[2] **TITLE:**Secure keyword search and data sharing mechanism for cloud computing.
AUTHOR:C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski, and L. Fang.
YEAR: 2023
DESCRIPTION: 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. Finally, the proposed construction is demonstrated practical and efficient in the performance and property comparison.

[3]**TITLE:**Omnes pro uno: Practical multi-writer encrypted database
AUTHOR:J. Wang and S. S. Chow
YEAR: 2022
DESCRIPTION: 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

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

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.

III. SYSTEM ARCHITECTURE

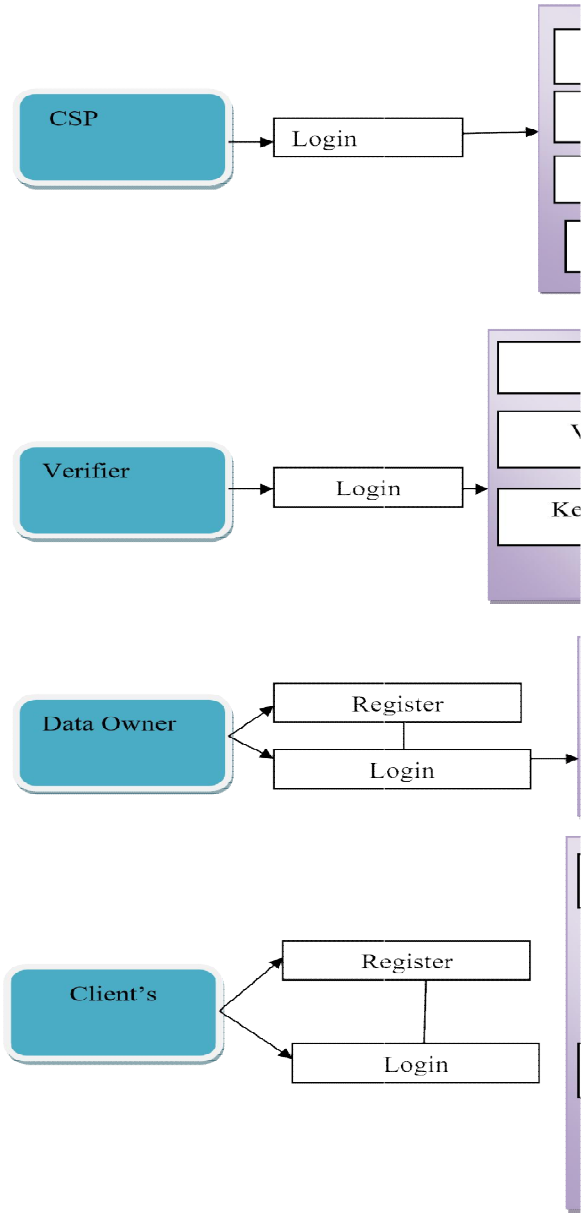

Fig: System Architecture

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

2.1 **Methodologies**

2.1.1 **Module Overview**

This project having the following 5 modules:

- User interface design
- Csp
- Verifier
- Data owner
- Client

2.1.2 **Module Descriptions**

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.

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.

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

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.

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.

2.2 Technique

We have conducted experiments on our collected dataset and extensive results have demonstrated that our model outperforms all other existing models. In the future, we will investigate more tasks under this framework, such as event summarization and event attribute mining in social media.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

Design and Workflow modeling

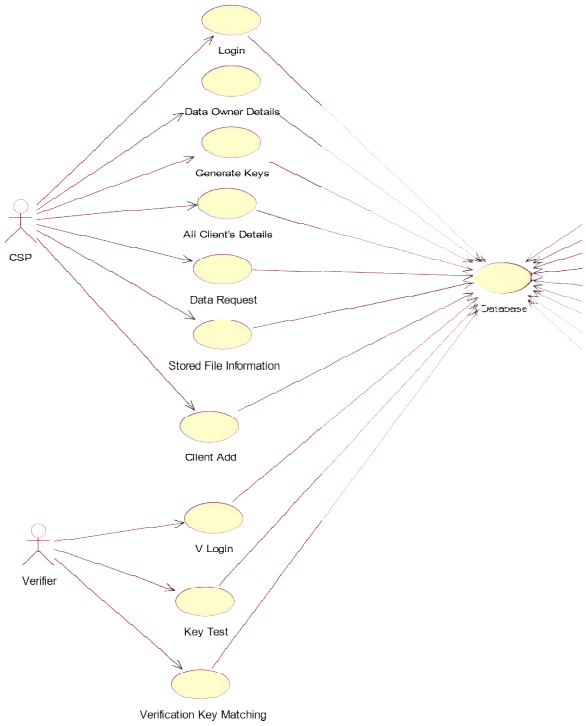

Fig. USE CASE DIAGRAM

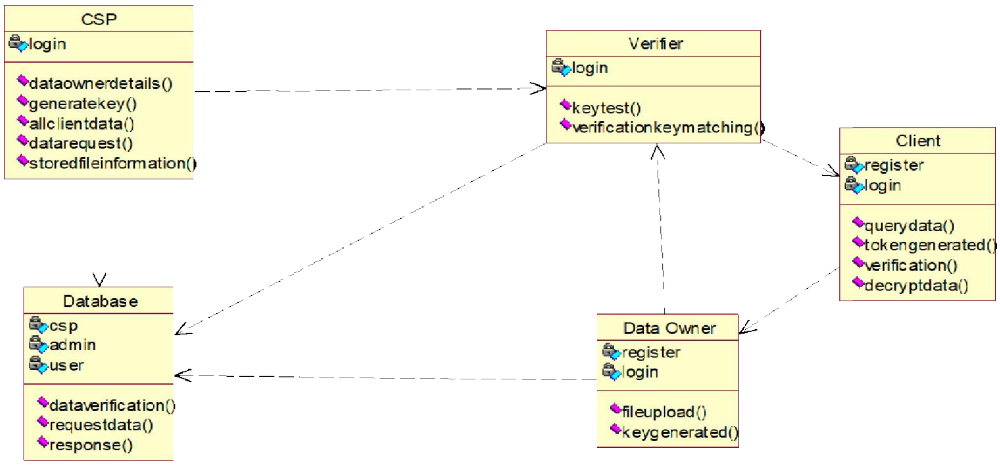

Fig. CLASS DIAGRAM

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

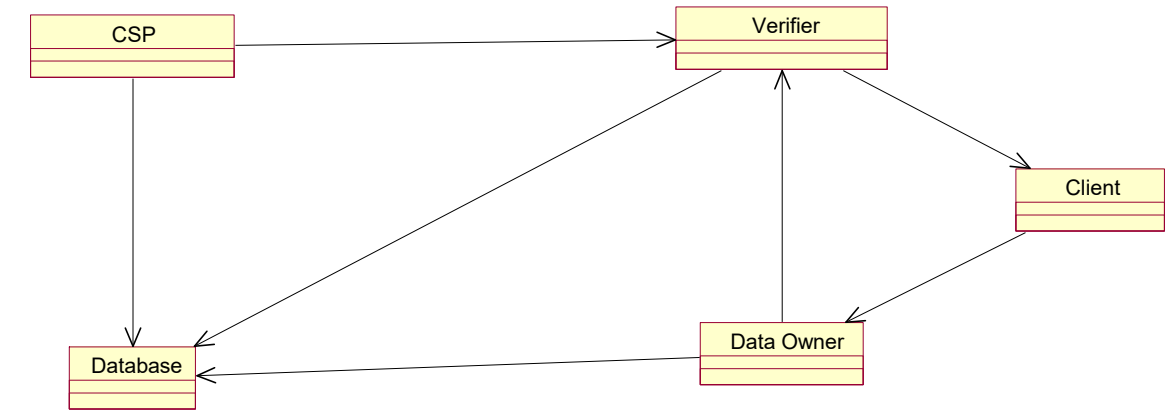

Fig. OBJECT DIAGRAM

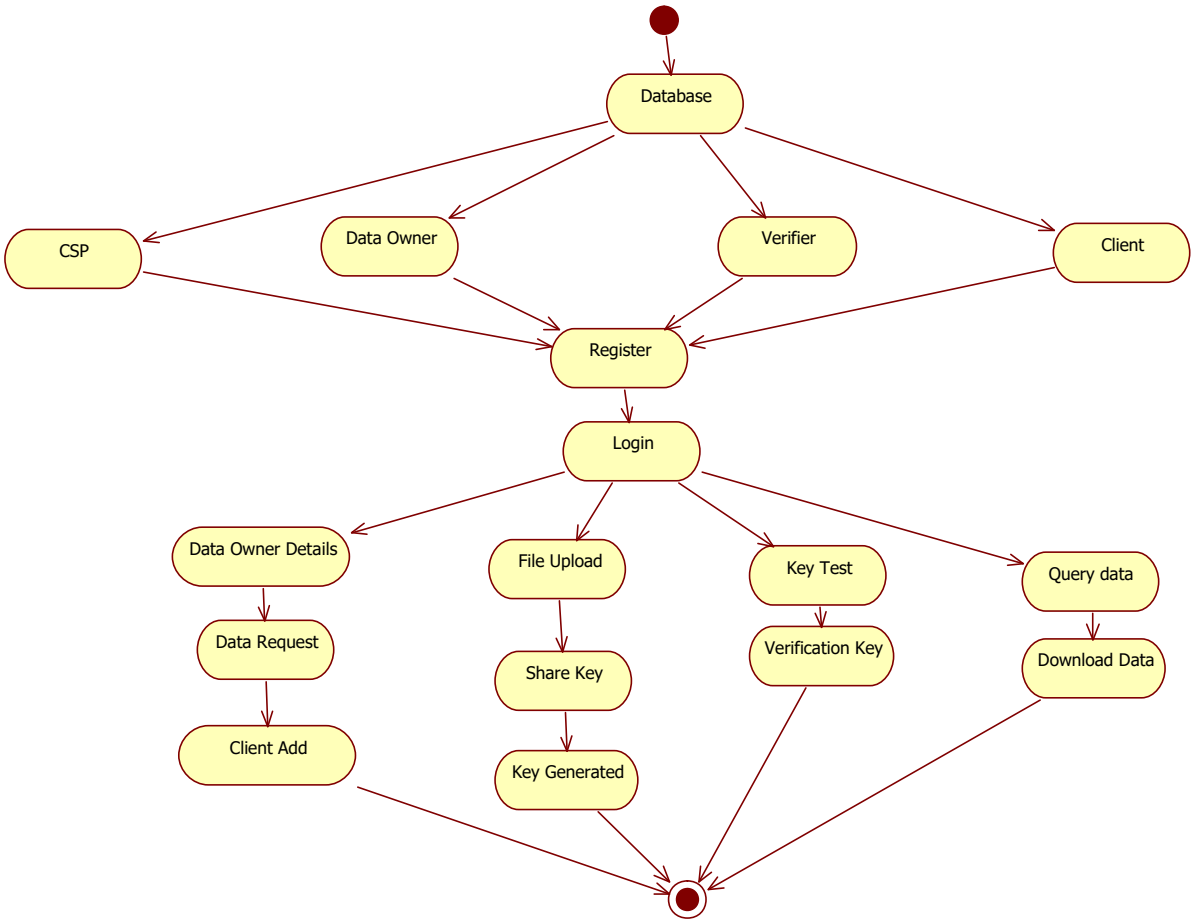

Fig. ACTIVITY DIAGRAM

Design Engineering deals with the various UML(Unified Modeling Language) diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software.

In the USE CASE DIAGRAM, The primary objective of a use case diagram is to demonstrate the existence of an actor who functions as a data user, a data owner, and a cloud server. Various types of actions are executed. The actor acting as the data user performs actions like searching files, viewing responses, and viewing search keywords.

In CLASS DIAGRAM, it represents how the classes with attributes and methods are linked together to perform the verification with security. From the above diagram shown the various classes involved in our project.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

In OBJECT DIAGRAM, it tells about the flow of objects between the classes. It is a diagram that shows a complete or partial view of the structure of a modeled system. In this object diagram represents how the classes with attributes and methods are linked together to perform the verification with security.

In ACTIVITY DIAGRAM, are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency.

III. RESULTS AND DISCUSSION

This project is implements like web application using COREJAVA and the server process is maintained using the SOCKET & SERVERSOCKER and the design part is played by cascading style sheet.

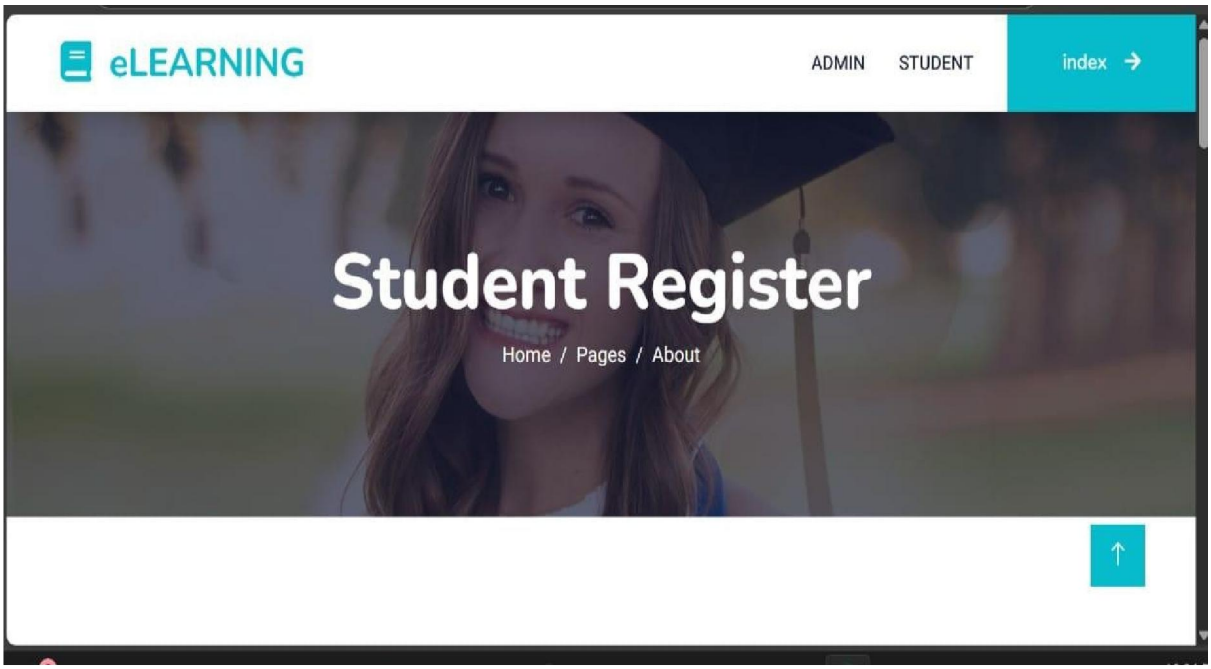

Fig.1.1 eLearning

Fig.1.2 Admin Login

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

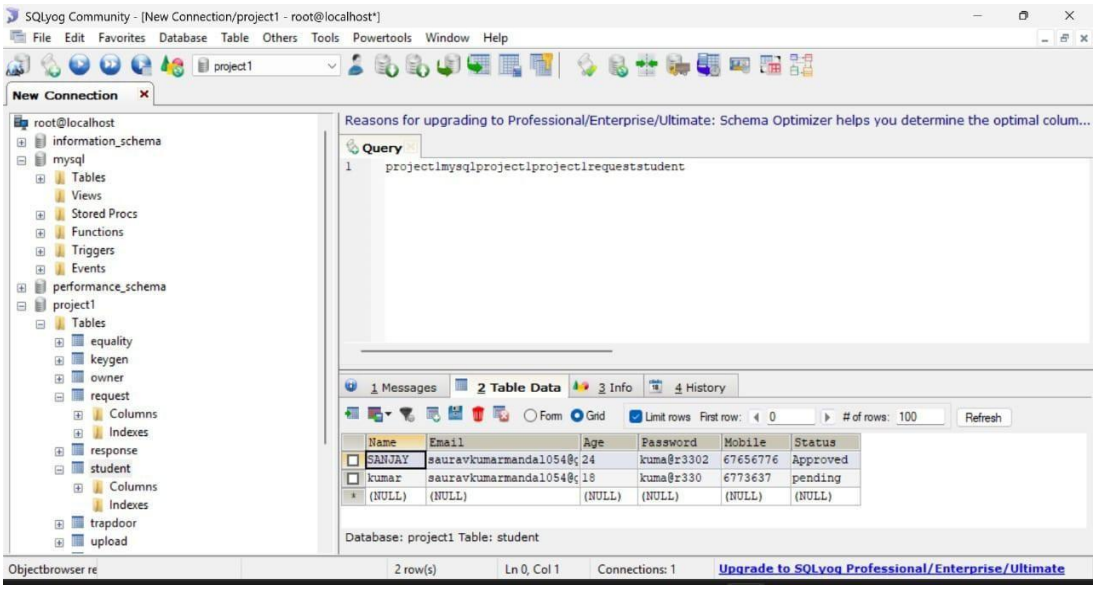

Fig.1.3 Database in SQL

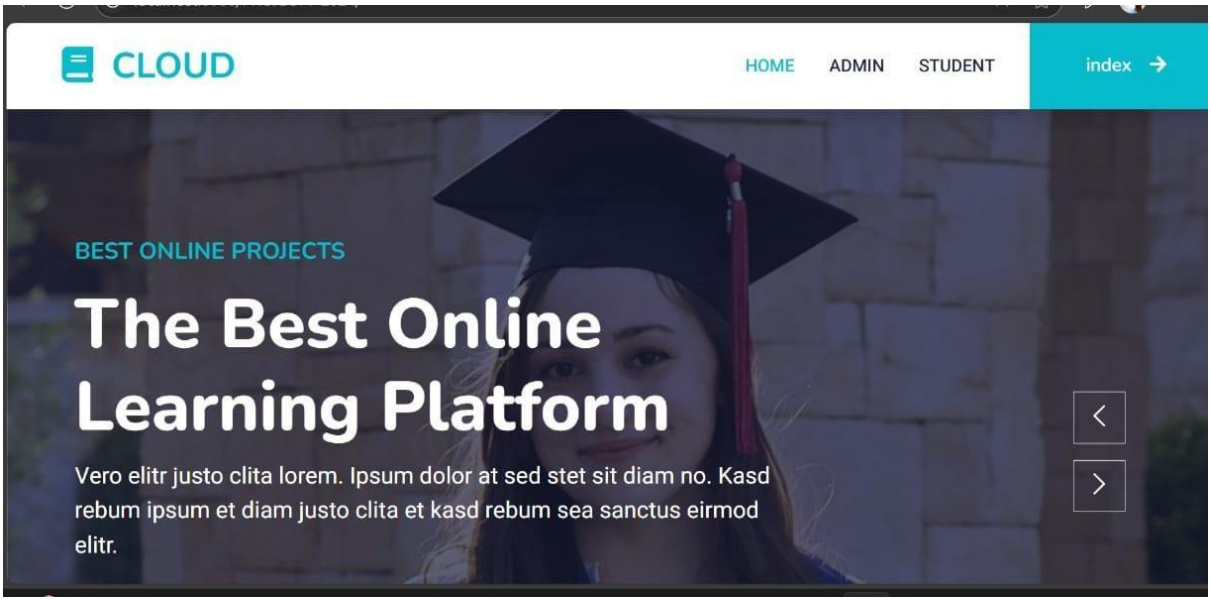

Fig.1.4 Home Page

IV. CONCLUSION AND FUTURE SCOPE

In this paper, 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.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

Finally, we formally analyzed the security of our proposed schemes and conducted extensive experiments to show their effectiveness. For future work, we intend to enhance the security and performance of PVAKSE further.

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-butcurious cloud servers," in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2012, pp. 917–922.