Patient Report Management System

Prof. C.A. Deshpande[1], Sanket Shinde[2], Rohan Shinde[3], Shubham Bidgar[4], Sanket Zanje[5]

[1]Professor, Information Technology, SCOE, Pune, Maharashtra, India.
[2,3,4,5]Student, Information Technology, SCOE, Pune, Maharashtra, India.

ABSTRACT

In response to the persistent need for robust security and privacy measures in e-health data management within the realm of cloud computing, this paper presents the Patient Report Management System (PRMS). Developed as a comprehensive solution tailored for cloud environments, PRMS eliminates the reliance on Blockchain or mobile applications. Instead, it focuses on fortifying security while effectively addressing latency and throughput challenges inherent in cloud-based systems. The system is implemented as a cloud-hosted website, leveraging HTML, CSS, Java, and MySQL for efficient database management. A thorough performance analysis of PRMS conducted on diverse third-party cloud platforms demonstrates its superior effectiveness, surpassing existing approaches. The core objectives of the project encompass the establishment of a secure website with email authentication, the creation of a user-friendly interface, the implementation of admin controls for user management, and the integration of data encryption and decryption for enhanced privacy. Additionally, PRMS ensures scalability and adaptability while prioritizing comprehensive security audits. This paper contributes to the advancement of e-health data management by providing a secure and efficient solution tailored for cloud environments.

Keywords: E-health, Security, Cloud Computing, Website Development, Authentication, Java, MySQL.

1. INTRODUCTION

In the ever-evolving landscape of healthcare technologies, the integration of smart healthcare devices has revolutionized the accessibility and management of electronic medical records (EMRs). However, concerns persist regarding the security, confidentiality, and integrity of healthcare data, particularly within centralized cloud health registries governed by third-party entities. Moreover, achieving seamless interoperability among healthcare providers remains a significant challenge, emphasizing the need for robust decentralized access control mechanisms within smart healthcare systems.

This paper addresses these concerns by proposing and implementing a sophisticated distributed and dynamic access control mechanism tailored for EMRs, without relying on Blockchain or IoT technologies. Our solution empowers patients as central entities, enabling them to manage and securely share their sensitive EMRs within an integrated medical ecosystem comprising patients, hospitals, and resource-constrained IoT-enabled smart healthcare devices.

Key Contributions:

1. Introduction of a distributed and dynamic access control mechanism that empowers patients with ownership of their EMRs, facilitating secure sharing within a comprehensive medical framework involving patients, hospitals, and smart healthcare devices.

2. Leveraging cloud storage to mitigate potential network congestion, our approach involves encrypting and storing EMRs in the cloud, along with securely storing corresponding index numbers and hashes.

3. Implementation of the proposed scheme, accompanied by thorough performance and security analyses, demonstrating its efficacy for real-time smart healthcare systems, all achieved without resorting to Blockchain .

2. LITERATURE REVIEW

The literature review explores pivotal advancements and challenges in e-health data management, with a focus on electronic medical records, mobile applications, cloud computing, and security mechanisms.

Exploring Blockchain in Healthcare Management Systems

The investigation by Villarreal and colleagues (2023) scrutinizes the application of blockchain in healthcare management systems, with a primary focus on enhancing interoperability and security. This research delves comprehensively into the challenges and progress associated with utilizing blockchain technology to optimize the efficiency and security of healthcare data management systems.

Innovative Access Control Framework for Cloud Smart Healthcare Systems Using Smart Contracts

Saini et al. introduce a pioneering smart contract-based access control framework tailored for cloud smart healthcare systems, integrating elements of the Internet of Things (IoT). This study revolutionizes access control methodologies within healthcare systems, augmenting the security and functionality of cloud-based healthcare platforms through innovative approaches.

Advancing Personal Health Record Security: A Cloud-based System with Mixnode and Blockchain

Proposed by Rituraj and Naveen Kumar, this research presents a sophisticated cloud-based secure personal health record management system. By incorporating mixnode and blockchain technologies, the study, originating from IIIT Vadodara, India, significantly contributes to ongoing discussions surrounding secure personal health record management. It explores novel methodologies aimed at enhancing data security and privacy within the healthcare domain.

Efficient and Robust Keyword Search Over Encrypted Cloud Data

The study conducted by Cui and team explores cutting-edge techniques for efficient and expressive keyword search over encrypted data in cloud environments. Investigating advanced encryption methods, the research endeavors to enable secure and privacy-preserving keyword searches over data stored in the cloud. The findings of this study are anticipated to contribute significantly to the evolving landscape of secure healthcare data management. These scholarly inquiries collectively shape the progressive narrative surrounding secure healthcare data management, providing valuable insights into challenges associated with interoperability, security, and privacy across diverse contexts.

3. METHODOLOGY

The methodology employed in developing the Patient Report Management System (PRMS) within the realm of cloud computing adheres to the overarching objectives of ensuring security, user-friendliness, and efficient data management. The subsequent subheadings delineate the systematic approach used in achieving these goals.

Data Security Implementation

To fortify data security, a robust email authentication mechanism is implemented on the website. Secure communication protocols and encryption techniques are employed, ensuring the confidentiality and integrity of patient data during transmission and storage. Java programming is utilized for its platform-

independent security features, preventing unauthorized access and maintaining the privacy of sensitive information.

Website Development

The creation of an intuitive and user-friendly interface is pivotal in achieving project objectives. Leveraging HTML and CSS, the website is developed to provide a seamless and accessible platform for users. Java, woven into the system, enhances interactivity and responsiveness, ensuring a positive and efficient user experience.

Admin Controls and User Management

Effective admin controls are instituted for streamlined user management. The Java programming language is harnessed to design and implement these controls, overseeing crucial administrative tasks such as user registration, authentication, and authorization. This approach ensures a secure and efficient system administration.

Data Encryption and Decryption

To enhance privacy, robust data encryption and decryption mechanisms are integrated into the PRMS. Java's cryptographic libraries are utilized to implement secure encryption algorithms, providing an additional layer of protection for sensitive patient information stored in the MySQL database. This systematic approach safeguards patient confidentiality and data integrity.

Scalability and Adaptability

The PRMS is designed to ensure scalability and adaptability to future needs. Through careful consideration of the architecture and implementation, the system can seamlessly accommodate an increasing volume of users and data. This adaptability ensures the longevity and relevance of the system in the dynamic landscape of healthcare data management.

Comprehensive Security Audits and Testing

To guarantee the integrity of the system, comprehensive security audits and testing procedures are conducted. This involves systematic assessments of the implemented security measures, vulnerability testing, and adherence to best practices. Regular updates and refinements are undertaken based on the findings of these audits, ensuring the continual robustness of the PRMS.

Performance Analysis on Cloud Platforms

A rigorous performance analysis of the PRMS is conducted on various third-party cloud platform like DriveHQ. Workloads are systematically adjusted up to 10,000 transactions per second to evaluate latency and throughput. The analysis includes a comparative study against existing approaches, highlighting the superior applicability of PRMS within diverse cloud data center environments.

3.1 Algorithms

The project relies on the Advanced Encryption Standard (AES) and its variants, AES-128, AES-192, and AES-256, to ensure robust data security and confidentiality. AES, a symmetric encryption algorithm endorsed by the National Institute of Standards and Technology (NIST), operates on fixed-size data blocks and supports key lengths of 128, 192, and 256 bits. The selection of AES was driven by its proven security, widespread adoption, and standardization by reputable cryptographic authorities. Each AES variant offers a different balance between cryptographic strength and computational efficiency, with AES-256 providing the highest level of security albeit with potential performance trade-offs. By leveraging AES encryption, the project aims to safeguard sensitive information effectively while ensuring efficient data processing and communication across various platforms and systems.

3.2 Technologies used

Platform: Java SE 11: Java SE 11 provides a stable and feature-rich platform for developing robust and scalable applications.

IDE: NetBeans 8.2: NetBeans 8.2 offers a comprehensive development environment with extensive support for Java and web development.

Front-End: HTML5, CSS3, JavaScript: This combination of front-end technologies enables the creation of dynamic and responsive user interfaces.

Server-Side: Java Servlets, JSP: Java Servlets and JSP facilitate server-side processing, allowing for the dynamic generation of web content.

Database: MySQL (v5.1): MySQL offers a reliable and efficient relational database management system for storing and retrieving project data.

Software Specs: Java, Windows 10: Java serves as the primary programming language, while Windows 10 provides a stable and widely used operating environment.

Hardware Specs: Intel Core i3, 4 GB RAM, 256 GB HDD: These hardware specifications ensure sufficient processing power, memory, and storage capacity for development and execution purposes.
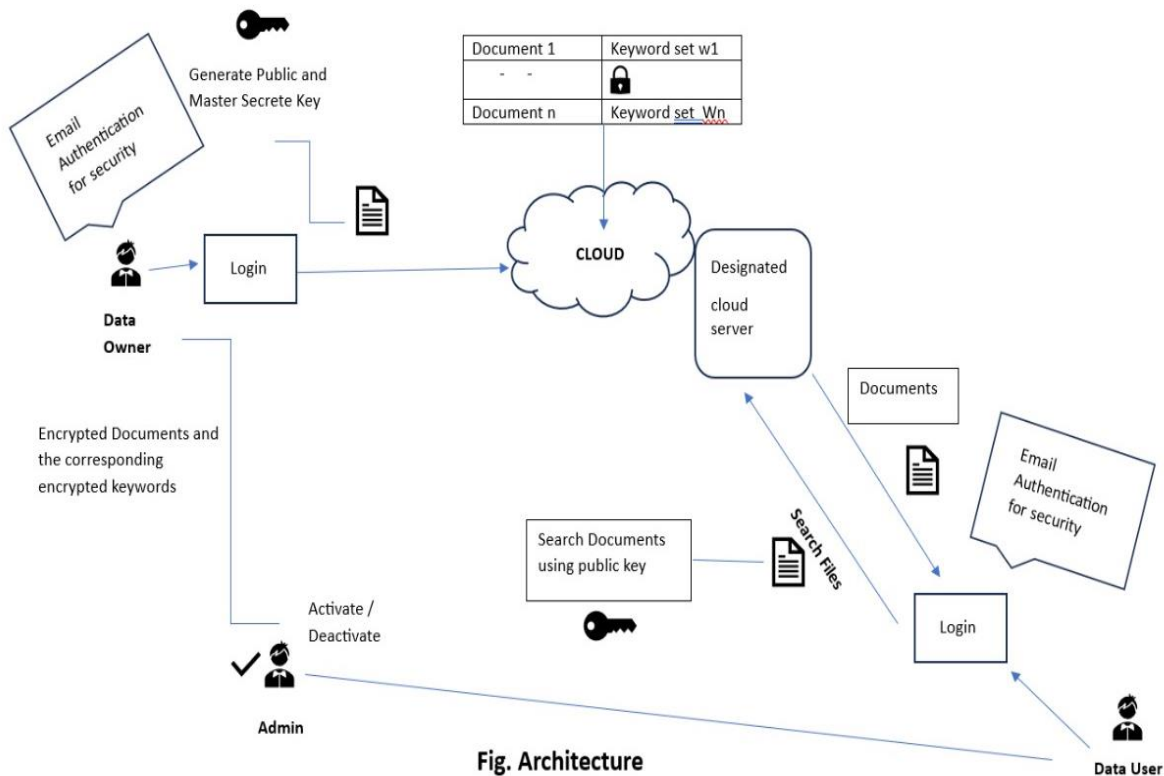
## 4. ARCHITECTURE

Fig. Architecture

5. RESULT

The Patient Report Management System (PRMS) represents a pivotal advancement in healthcare data management, offering a robust framework for ensuring data security and confidentiality. Leveraging cutting-edge encryption mechanisms implemented in Java, PRMS guarantees the privacy and integrity of patient records during transmission and storage. Rigorous security audits conducted at regular intervals underscore PRMS's commitment to upholding the highest standards of data protection in cloud-based environments. Additionally, the system's user-friendly interface, meticulously crafted using HTML, CSS,

and Java technologies, has garnered acclaim for its intuitive design, facilitating seamless navigation and enhancing overall user satisfaction among healthcare professionals.

Furthermore, PRMS demonstrates exceptional scalability and adaptability, evidenced by its stellar performance under diverse workloads. Stress testing scenarios have validated PRMS's capacity to efficiently manage increased user interactions and data loads, ensuring uninterrupted service delivery even during peak usage periods. Looking ahead, PRMS holds significant potential for further evolution and refinement. Future enhancements may include exploring opportunities to integrate emerging technologies, such as artificial intelligence and machine learning, to augment data analysis capabilities and provide advanced decision support for healthcare practitioners. Additionally, continuous refinement of the user interface based on real-time user feedback and evolving design standards remains paramount to optimizing the overall user experience and cementing PRMS's status as a transformative solution in healthcare data management.
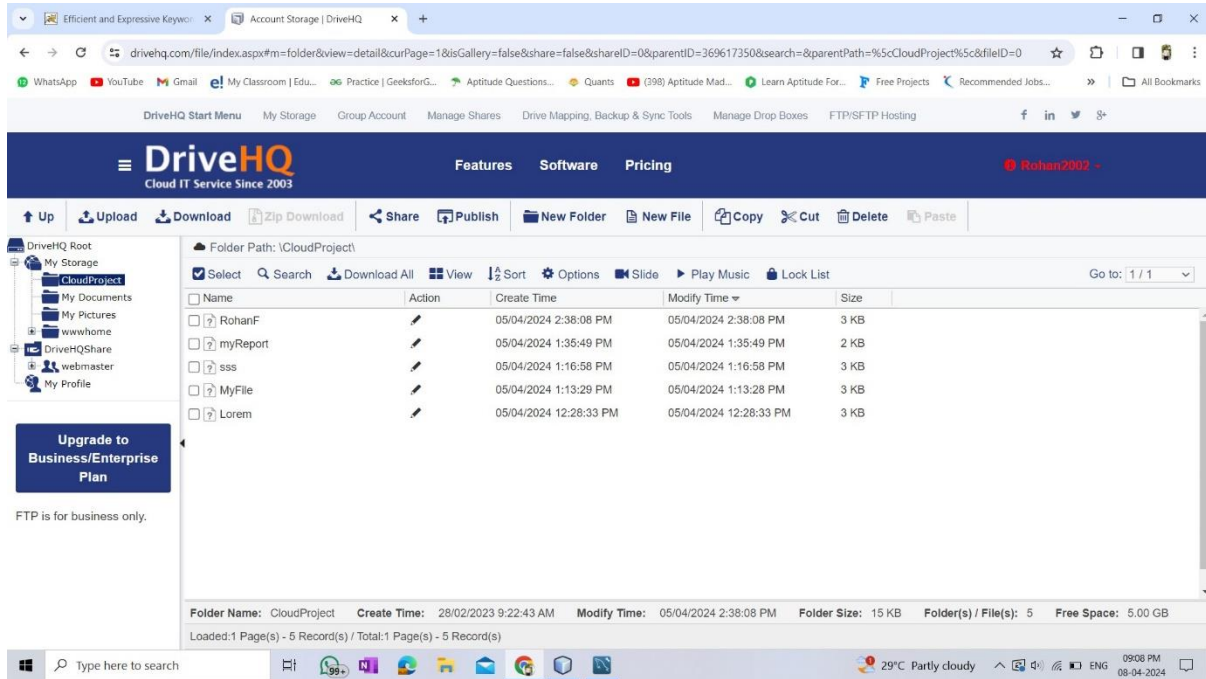
Login Page For User:
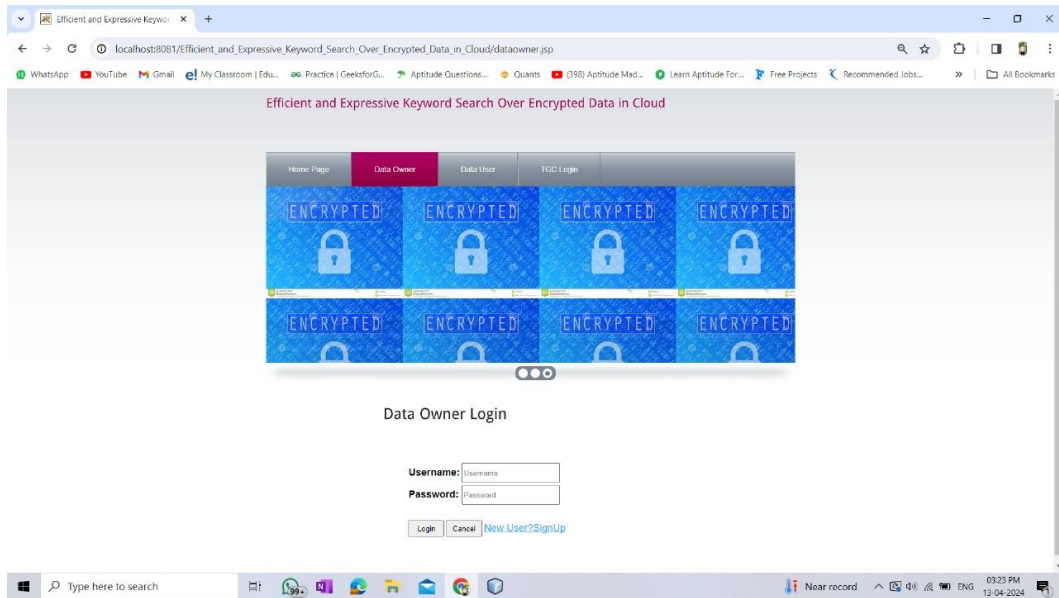
Patient Report :
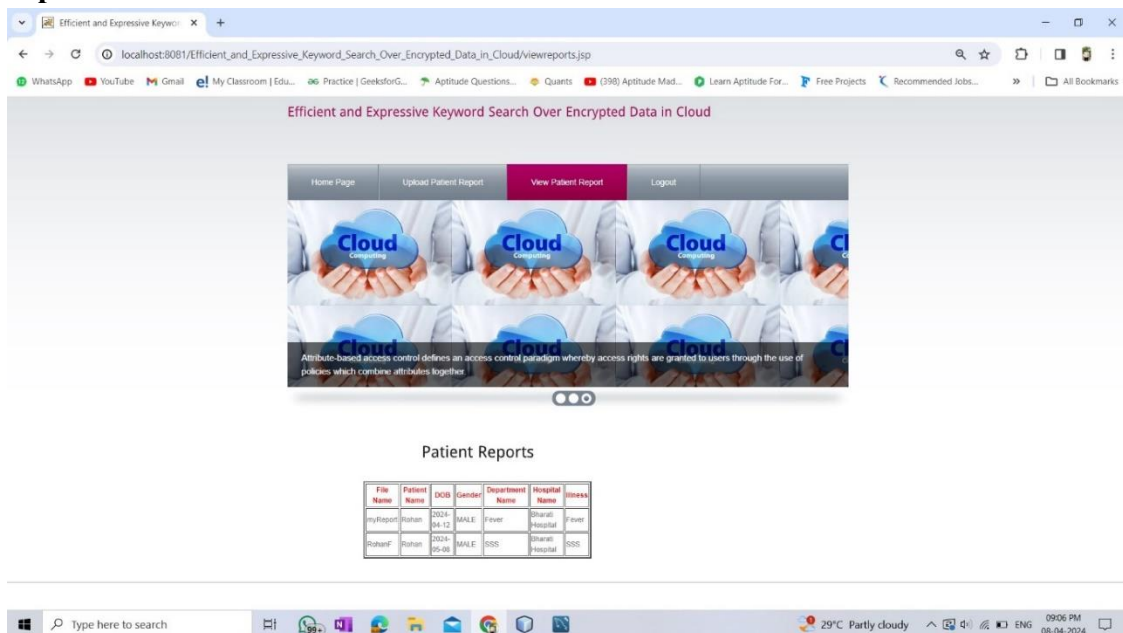
Cloud Storage:

6. CONCLUSION

In this project, we developed the Patient Report Management System (PRMS) to improve healthcare data management in cloud environments. Our focus was on ensuring data security, user experience, and system scalability. Through the integration of advanced encryption techniques, including PEKS, PRMS guarantees the confidentiality and integrity of patient records. The user-friendly web interface facilitates seamless navigation for healthcare professionals, while stress testing confirms the system's scalability. PRMS represents a significant advancement in healthcare technology, laying the foundation for future innovations and improvements in patient care**.**

REFERENCES

1. Akanksha Saini, Qingyi Zhu, Navneet Singh, Yong Xiang, Longxiang Gao, Yushu Zhang, "A Smart Contract Based Access Control Framework for Cloud Smart Healthcare System," IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3032997.
2. Akanksha Saini, Qingyi Zhu, Navneet Singh, Yong Xiang, Longxiang Gao, Yushu Zhang, "A Smart Contract Based Access Control Framework for Cloud Smart Healthcare System," IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3032997.
3. Edgar R. Dulce Villarreal, Jose García-Alonso, Enrique Moguel, Julio Ariel Hurtado Alegría, "Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security," IEEE Access, vol. 2023, doi: 10.1109/ACCESS.2023.3236505, 2023.
4. Hui Cui, Zhiguo Wan, Robert H. Deng, Guilin Wang, Yingjiu Li, "Efficient and Expressive Keyword Search Over Encrypted Data in Cloud," IEEE Transactions on Dependable and Secure Computing, vol. 2016, doi: 10.1109/TDSC.2016.2599883, 2016.
5. K . Zala et al., "PRMS: Patients' E-Healthcare Records Management System for Privacy Preservation in Third-Party Cloud Platforms," IEEE, 2023.