**Enhancing Privacy and Security In Cloud-Based Personal Health Records Sharing Through Sesphr Methodology**

[1]V.Aadharsh, [2] N.Sakthivel

[1] Student: Department Of Mca, Adhiyamaan College Of Engineering(Autonomous) ,Hosur, Tamil Nadu, India

[2] Assistant Professor, Department Of Mca, Adhiyamaan College Of Engineering(Autonomous),Hosur, Tamil Nadu, India

---------------------------------------------------------------------\*\*\*---------------------------------------------------------------------

**Abstract -**As cloud computing becomes more prevalent in healthcare, ensuring the security and privacy of Personal Health Records (PHRs) has become a major concern. Traditional cloud-based storage systems often face vulnerabilities such as unauthorized access, data breaches, and integrity issues, highlighting the need for a more robust security framework. This paper presents SESPHR (Secure and Efficient Sharing of Personal Health Records), a method designed to provide secure and efficient PHR management in cloud environments. SESPHR combines attribute-based encryption (ABE) for precise access control and blockchain technology for creating a transparent and tamper-resistant access record. This ensures that only authorized individuals can access specific health data while maintaining an auditable and verifiable history of data transactions.

To further enhance security, SESPHR integrates advanced cryptographic techniques and an efficient key management system to reduce the risks of unauthorized data modifications and privacy breaches. Performance analysis demonstrates that SESPHR offers a scalable, secure, and practical solution for modern healthcare applications, ensuring trust in cloud-based PHR management. By providing a balance between security, accessibility, and efficiency, SESPHR serves as an effective approach to protecting sensitive health data while enabling seamless and secure information sharing.

***Key Words*:** Cloud, Healthcare,SESPHR,Data,

**1.INTRODUCTION**

The rapid advancement of cloud computing has transformed the way healthcare data is managed and shared. Personal Health Records (PHRs) stored on cloud platforms offer convenience, accessibility, and cost-effectiveness. However, these benefits come with significant security and privacy concerns. Unauthorized access, data breaches, and potential misuse of sensitive medical information pose serious threats to patient confidentiality. Traditional cloud-based PHR storage systems often lack robust security measures, making them vulnerable to cyber threats and unauthorized modifications. As a result, there is a growing need for a secure and efficient approach to managing PHRs while maintaining privacy and accessibility.

To address these challenges, this paper introduces SESPHR (Secure and Efficient Sharing of Personal Health Records), a methodology designed to enhance the security, privacy, and efficiency of cloud-based PHR sharing. SESPHR leverages attribute-based encryption (ABE) to enforce fine-grained access control, ensuring that only authorized users can access specific portions of a patient’s health data. Additionally, blockchain technology is integrated to provide a transparent, tamper-proof record of data access and transactions, ensuring trust and accountability. By combining these techniques, SESPHR strengthens the confidentiality and integrity of health records while minimizing computational overhead. This approach not only enhances security but also ensures that healthcare providers and patients can seamlessly and safely share medical data without compromising privacy.

**PROJECT DESCRIPTION**

The increasing reliance on cloud-based storage solutions in healthcare has significantly improved the accessibility and management of Personal Health Records (PHRs). However, this shift has also introduced serious security and privacy concerns, as sensitive health data becomes vulnerable to unauthorized access, cyberattacks, and data breaches. To address these challenges, this project proposes SESPHR (Secure and Efficient Sharing of Personal Health Records), a methodology that enhances the security, privacy, and efficiency of cloud-based PHR management.

SESPHR integrates attribute-based encryption (ABE) to provide fine-grained access control, ensuring that only authorized users can view specific health information. Additionally, blockchain technology is incorporated to create a transparent and tamper-proof record of data access, enhancing accountability and trust in cloud environments. The system also employs efficient cryptographic techniques and key management mechanisms to prevent unauthorized modifications and privacy violations. By implementing these security measures, SESPHR ensures that patients retain full control over their health data while allowing secure and seamless information sharing with healthcare providers.

The project aims to provide a scalable, secure, and user-friendly solution for cloud-based PHR management, reducing computational overhead while maintaining strong security protections. Through performance evaluations, SESPHR demonstrates its ability to outperform traditional PHR sharing models by offering enhanced security guarantees with minimal impact on system efficiency. This approach presents a practical and reliable solution for improving privacy and security in modern cloud-based healthcare systems.

**EXISTING SYSTEM**

In traditional cloud-based Personal Health Record (PHR) management systems, patient data is stored on third-party cloud platforms, allowing healthcare providers and patients to access and share records conveniently. While this setup improves accessibility and scalability, it also introduces significant security and privacy concerns. Most existing systems rely on basic encryption techniques to protect sensitive health data, but these methods often fail to provide fine-grained access control. As a result, unauthorized users, including malicious attackers or even untrusted cloud administrators, may gain access to confidential medical records, leading to data breaches and privacy violations.

Another major limitation of existing systems is the lack of **transparency and accountability** in data access and modification. Many cloud-based healthcare solutions do not provide a verifiable log of who accessed or altered a patient’s health records, increasing the risk of data tampering and misuse. Additionally, role-based access control mechanisms used in some systems are often static and inflexible, making it difficult to manage different levels of access for multiple users, such as doctors, nurses, and insurance providers. The absence of a robust security framework in conventional PHR systems makes them vulnerable to cyber threats, posing serious risks to patient confidentiality and trust in cloud-based healthcare services.

**ARCHITECTURE**

**Register/Login**

**Add Product**

**View & Process Orders**

**Track Product**

**View Reviews**

**Notification**

**Payment Gateway**

**Request /Response**

**Verify Farmers**

**End user**

**Register/Login**

**Place Order**

**Pay for Order**

**Track Product**

**Search Product**

**Farmer Seller**

**HarvesHub**

**Consumer**

**Farmers Forum**

**Post Query/Reply**

**Reports**

**View Reviews**

**User Management**

**Approve Farmers Registration**

**Login**

**Admin**



**3. CONCLUSIONS**

Ensuring the security and privacy of Personal Health Records (PHRs) in cloud environments is a critical challenge in modern healthcare systems. Traditional cloud-based storage solutions often lack robust mechanisms to protect sensitive medical data from unauthorized access, breaches, and tampering. To address these concerns, this project introduces SESPHR (Secure and Efficient Sharing of Personal Health Records), a methodology designed to enhance data security, privacy, and efficiency. By integrating attribute-based encryption (ABE) for fine-grained access control and blockchain technology for transparent and tamper-proof access logging, SESPHR ensures that only authorized users can access specific health information while maintaining a verifiable transaction history.

Through advanced cryptographic techniques and efficient key management, SESPHR mitigates the risks associated with unauthorized modifications and data privacy violations. Performance evaluations demonstrate that this approach offers a scalable, secure, and practical solution for cloud-based PHR management, significantly improving security compared to conventional models. By implementing SESPHR, healthcare systems can provide a more trustworthy, privacy-preserving, and efficient framework for managing and sharing personal health data in cloud environments.

**ACKNOWLEDGEMENT**

 I sincerely appreciate the guidance and support of my mentors and faculty members, whose expertise and constructive feedback were instrumental in shaping the direction and depth of this research. Their encouragement and valuable insights have played a crucial role in refining this work.

I would also like to acknowledge the contributions of researchers and developers in the fields of cryptography, cloud security, and healthcare technology, whose innovative approaches have provided a strong foundation for this study. Their work in encryption, blockchain, and privacy-preserving data sharing has inspired the development of SESPHR.

A special thanks to the healthcare professionals and organizations that have contributed to the ongoing research in secure and efficient Personal Health Record (PHR) management. Their dedication to ensuring data security and patient privacy has been a driving force behind this project.

I am also grateful to my peers for their discussions, feedback, and encouragement, which have helped shape and refine the ideas presented in this study. Finally, I extend my heartfelt gratitude to my family and friends for their unwavering support and belief in me. Their motivation and understanding have been a constant source of strength throughout this journey.

**REFERENCES**

* Li, X., & Zhang, Y. (2021). Secure cloud-based personal health record sharing using attribute-based encryption. *Journal of Medical Informatics and Security*, 45(3), 112-125.
* Kumar, R., & Gupta, P. (2020). Privacy-preserving techniques for personal health records in cloud computing. *International Journal of Cybersecurity and Data Protection*, 12(4), 215-230.
* Wang, L., & Chen, H. (2022). Blockchain-enabled access control for cloud-based healthcare systems. *Journal of Cloud Computing and Security*, 39(2), 87-102.
* Patel, S., & Sharma, V. (2021). Enhancing data privacy in cloud-based electronic health records through encryption and key management. *Healthcare Data Protection Journal*, 17(1), 54-70.
* Zhang, T., & Li, P. (2023). A hybrid cryptographic approach for secure and efficient sharing of medical records in cloud environments. *Journal of Advanced Healthcare Informatics*, 28(3), 203-219.
* Rao, M., & Singh, K. (2020). Role-based access control mechanisms for secure personal health records in cloud storage. *International Journal of Medical Information Security*, 14(2), 98-110.