International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Securing Government Healthcare Services Through a G-Cloud Based Framework

T.SRAVANTHI(ASSISTANT PROFESSOR), **CH.V ASHRITA KUSUMA**(ENGINEERING STUDENT), **K.YASHWANTH**(ENGINEERING STUDENT), **K.BHARGAV**(ENGINEERING STUDENT), **B.JITHENDRA**(ENGINEERING STUDENT)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SANKETIKA VIDYA PARISHAD ENGINEERING COLLEGE

VISAKHAPATNAM, INDIA

ABSTRACT

Nowadays, cloud computing is gaining significant attention for data storage and access, catering to users ranging from small-scale businesses to large enterprises. In the healthcare sector, the demand for cloud-based solutions is particularly high, as they enable efficient storage and retrieval of patient records. However, current cloud servers used in government healthcare services often lack complete security and flexibility.This project proposes a flexible, secure, cost-effective, and privacy-preserving cloud-based framework for healthcare systems. Specifically, we introduce a secure and efficient framework for the government Electronic Health Record (EHR) system, incorporating multi-authority attribute-based encryption (MABE) within a hierarchical structure to enforce robust access control policies.

1. INTRODUCTION

A common challenge in the healthcare sector across many countries is the suboptimal utilization of available human and material resources, which hinders the delivery of integrated healthcare aimed at both disease prevention and treatment. Statistics show that Arab countries experience high rates of health issues such as diabetes, liver disease, and parasitic infections like schistosomiasis and malaria. Many of these conditions could be mitigated or their complications reduced through early detection and preventive measures. However, several factors—including planning, operational, and technical challenges—impede progress. Overcoming these obstacles could significantly enhance the quality of healthcare services. Additionally, there is a notable weakness and scarcity of hospital information systems, which are among the most advanced tools designed to streamline technical and administrative healthcare operations. These systems play a crucial role in enabling medical institutions to maintain full control over their resources and activities. However, their success does not solely depend on selecting the right hardware and storage software. Instead, their effectiveness relies on their adaptability to various users—including doctors, nurses, technicians, and administrators—each of whom has different priorities, information needs, and expectations from these systems.

1.1 PROJECT PURPOSE

The traditional paper-based healthcare system has been replaced by electronic health information systems due to its inefficiency, which stemmed from limitations such as low storage capacity, high operating and maintenance costs, and challenges in system integration [1]. Subsequently, computerized health systems have transitioned to cloud computing, leveraging its more efficient infrastructure and numerous IT benefits, including cost-effectiveness, scalability, and flexibility [2].Cloud computing in electronic health records significantly reduces expenses related to healthcare services, maintenance, networking, licensing fees, and

infrastructure. This cost reduction serves as a strong incentive for developers to adopt cloud-based solutions in healthcare [2], [3]. However, the rapid shift toward cloud-based healthcare systems has raised concerns regarding critical issues such as privacy and information security [4], [5]. While cloud adoption allows healthcare providers to focus more on clinical and patient-related services rather than infrastructure management [6], it also introduces challenges related to the sharing of personal and health information over the Internet and external servers. These challenges include privacy risks, security vulnerabilities, access control issues, and regulatory compliance concerns [7], [8], [9], [10].

Despite extensive research on cloud computing in healthcare, there is currently no comprehensive framework that effectively addresses all viable models and interconnections between cloud technology and healthcare services [11], [12]. Several researchers have explored ways to enhance cloud-based healthcare frameworks [13], [14], [15], and further advancements in addressing these challenges will be crucial for increasing cloud adoption in healthcare. Continued improvements will encourage healthcare providers to fully embrace cloud-based solutions, ensuring more secure and efficient healthcare services [16].

1.2 PROJECT OVERVIEW

The exchange of personal and health information over the Internet and across various external servers, beyond the secure environment of healthcare institutions, has raised significant concerns regarding privacy, security, access control, and regulatory compliance [7], [8], [9], [10]. Existing research lacks a comprehensive framework that effectively addresses all potential models and interconnections between cloud computing and healthcare technology [11], [12]. While several studies have explored ways to enhance cloud-based healthcare frameworks [13], [14], [15], further advancements are necessary to overcome these challenges. Continued innovation in this area will drive wider adoption of cloud healthcare solutions and encourage healthcare providers to embrace cloud-based services more confidently [16].

2. LITERATURE SURVEY

INTRODUCTION

A literature survey is a crucial step in the software development process. Before developing a tool, it is essential to assess key factors such as time constraints, cost-effectiveness, and the available resources within a company. Once these aspects are evaluated, the next step involves selecting the appropriate operating system and programming language for development. During the implementation phase, programmers often require external support, which can be obtained from senior developers, reference books, or online resources. Considering these factors before system development ensures a well-structured and efficient approach to building the proposed solution.

RELATED WORK

Masrom, Maslin, and Ailar Rahimli [1] conducted a study titled A Review of Cloud Computing Technology Solutions for Healthcare Systems. Initially, traditional healthcare information systems relied on paper-based records, which were later replaced by Healthcare Information Systems (HIS). However, HIS was found to be inefficient due to several challenges, including limited storage capacity, difficulties in system integration, high operational costs, and complex maintenance requirements.

Cloud computing has emerged as a transformative technology, delivering software, infrastructure, and computational platforms as a service over the Internet, accessible anytime and anywhere. This innovation addresses many challenges in the healthcare sector, such as expanding storage capacity, enhancing system capabilities, and improving overall performance. Cloud computing provides cost-effective solutions, enhances interoperability and accessibility, optimizes resource utilization, and integrates healthcare information systems.

By resolving existing limitations, cloud computing enhances the functionality and efficiency of healthcare information systems. This study explores cloud computing as a solution to key challenges, including data transmission, storage, cost management, and system maintenance. Additionally, the implications of adopting cloud computing in healthcare are analyzed,

highlighting its potential to revolutionize healthcare information systems.

2.1 RELATED WORK

Anežka Hucíková [2] described cloud computing as a self-service, on-demand network access model that delivers computing resources and services efficiently. Recent studies indicate that nearly 50% of healthcare organizations, ranging from large hospitals to ambulatory services in the US and Europe, have already adopted cloud technology. As cloud computing continues to evolve, an increasing number of healthcare providers are expected to transition their enterprise communication to the cloud. However, there is a growing need for a deeper understanding of both the opportunities and challenges faced by technology providers and healthcare organizations. Additionally, the study suggests strategies to address specific challenges associated with cloud adoption in the healthcare sector.Yang, Haibo, and Mary Tate et al. [3] conducted a descriptive literature review and developed a classification scheme for cloud computing research. Their study analyzed 205 peer-reviewed journal articles published since the inception of cloud computing research, categorizing them into four main areas: technological issues, business considerations, application domains, and conceptual frameworks. The findings indicate that while research predominantly focuses on technological challenges, emerging themes related to social and organizational implications are gaining attention. This review serves as a valuable resource for information systems researchers, providing a structured classification of cloud computing literature while identifying gaps and potential future research directions.Dimitrios Lekkas et al. [4] explored how the emergence of cloud computing has reshaped infrastructure architectures, software delivery models, and development methodologies. Cloud computing integrates aspects of grid computing, utility computing, and autonomic computing into an innovative deployment model. However, this transition has raised significant concerns regarding communication and information security, which are critical to the success of information systems. The shift to cloud environments introduces new risks that traditional security mechanisms may not fully address.To mitigate these risks, the study proposes a security framework that integrates a Trusted Third Party (TTP) to ensure specific security standards within cloud environments. This solution leverages cryptographic techniques, specifically Public Key Infrastructure (PKI) combined with Single Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP), to enhance authentication, data integrity, and confidentiality. By establishing a horizontal security layer accessible to all stakeholders, this approach creates a security mesh that fosters trust and strengthens data protection in cloud-based healthcare systems.

3. EXISTING SYSTEM

In the current medical data-sharing systems, sensitive and valuable information is stored on cloud servers in plain text format. This lack of encryption leaves critical healthcare data vulnerable to security breaches and unauthorized access.

LIMITATIONS

- Traditional cloud servers and cloudlets are susceptible to attacks, allowing intruders to illegally access and retrieve sensitive data.
- Existing cloud systems do not support decentralized data access, limiting flexibility and security.
- There is no mechanism such as a Secret Authority (SA) to issue secure keys for government healthcare users, ensuring authorized and protected access to files.

4. PROPOSED SYSTEM

This project introduces a flexible, secure, cost-effective, and privacy-preserving cloud-based framework tailored for the healthcare sector. The proposed framework enhances security in government Electronic Health Record (EHR) systems by implementing multi-authority attribute-based encryption (MABE) within a hierarchical structure. This approach strengthens access control policies and ensures secure data sharing.

ADVANTAGES OF THE PROPOSED SYSTEM

The key benefits of the proposed system include:

- A highly efficient and authenticated security structure.

➢ The first practical mechanism offering robust protection against intruders attempting to access sensitive medical information.
➢ Theoretical and experimental results demonstrate the efficiency and effectiveness of the proposed framework in securing healthcare data.

5. SOFTWARE PROJECT MODULES

The implementation phase involves transforming the theoretical framework into a fully functional system. During this stage, the application is divided into multiple modules, each developed and tested for deployment.The proposed system is implemented using Java (JSE) to evaluate the performance of the security protocol. The application consists of the following four core modules:

1. Health Care providers (HCP) Module
2. Data User/patients Module
3. E-Cloud Service Module
4. Trusted Key Authority Module

Now let us discuss about each and every module in detail as follows:

5.1 HEALTHCARE PROVIDER MODULE

In this module, the Healthcare Service Provider (HCSP) or data owner uploads patient data to the cloud server. To ensure security, the data owner encrypts patient details before storage. The key functionalities in this module include:

- Upload Patient Details
- View All Uploaded Patient Records
- View Public Keys
- View Transaction Details

5.2 PATIENT/USER MODULE

In this module, users (patients) log in using their unique credentials (username and password). Upon successful login, users can search for patient records in the cloud based on indexed keywords and scores. The module provides the following operations:

- Search for Patients using Indexed Keywords
- Request Access Control from the Cloud Server
- Download Patient Records
- Request Key for Encrypted Files
- View Assigned Keys

5.3 E-CLOUD SERVER MODULE

The cloud server is responsible for managing data storage services. It stores encrypted patient data, facilitates secure sharing with remote users, and ensures data security. This module includes the following functionalities:

- View Healthcare Service Providers (HCSPs) and Patient Records
- Monitor and Manage Patient Details
- Track and Identify Potential Attackers
- Manage Patient Encryption Keys
- Un-Revoke Users (Restore Access to Previously Revoked Users)
- Monitor Transactions and Generate Reports
- Analyze Performance Metrics (Time Delay, Throughput, etc.)

5.4 TRUSTED KEY AUTHORITY MODULE

The Trusted Key Authority (TA) is responsible for managing encryption keys and ensuring secure access control. The key functionalities of this module include:

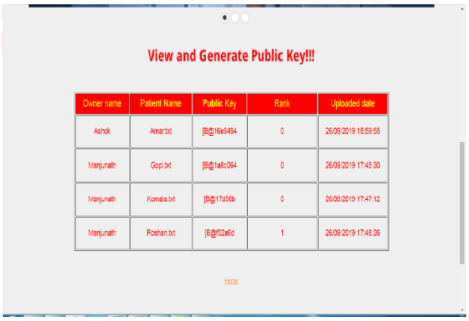
- View All Registered Patients
- Generate and Manage Public Key Requests
- Key Generation and Distribution

This modular architecture ensures a secure, efficient, and scalable cloud-based framework for managing electronic healthcare records while maintaining data privacy and integrity.

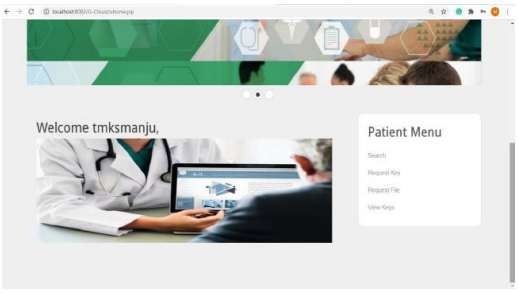
6. OUTPUT RESULTS

1) PKG CAN VIEW ALL PATIENTS DETAILS

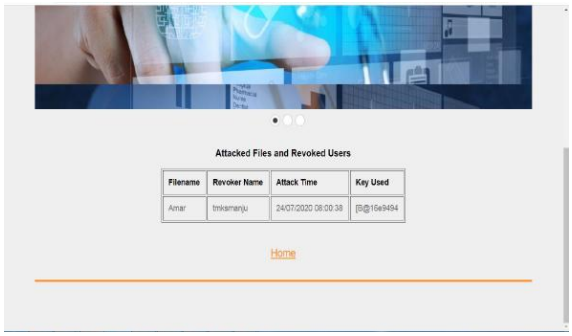
2) PKG CAN ABLE TO VIEW ALL PUBLIC KEYS



3) PATIENTS HOME PAGE:



4.USER CAN DOWNLOAD THE FILE BY SUBSTITUTING VALID DETAILS



7. CONCLUSION

In this work, we proposed a secure cloud-based Electronic Health Record (EHR) framework that ensures the security and privacy of medical data stored in the cloud. Our framework leverages hierarchical multi-authority Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enforce access control policies effectively.The proposed system enhances integration, interoperability, and secure data sharing among healthcare providers, patients, and practitioners. Within the framework, different attribute domain authorities manage specific attribute domains independently, reducing reliance on a centralized government authority and eliminating computational overhead. Additionally, the framework incorporates multi-factor authentication**,** ensuring robust security and verified access control.Our scheme is designed to be adaptable for governments with cloud computing infrastructures**,** enabling secure and efficient EHR management for public healthcare systems.Future work will focus on implementing and evaluating the proposed scheme in a real-world healthcare environment to further assess its performance and scalability.

8.REFERENCES

[1] Masrom, Maslin, and Ailar Rahimli. "A Review of Cloud Computing Technology Solution for Healthcare

System." Research Journal of Applied Sciences, Engineering and Technology 8, no. 20 (2014): 2150–2155.

[2] HUCÍKOVÁ, Anežka, and Ankica Babic. "Cloud Computing in Healthcare: A Space of Opportunities and

Challenges." Transforming Healthcare with the Internet of Things (2016): 122.

[3] Yang, Haibo, and Mary Tate. "A descriptive literature review and classification of cloud computing

research." CAIS 31 (2012): 2.

[4] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation

computer systems 28, no. 3 (2012): 583–592.

[5] Nigam, Vaibhav Kamal, and Shubham Bhatia. "Impact of Cloud Computing on Health Care." (2016).

[6] ―How to Improve Healthcare with Cloud Computing‖, By Hitachi Data Systems, white paper, (2012).

[7] Mehraeen, Esmaeil, Marjan Ghazisaeedi, Jebraeil Farzi, and Saghar Mirshekari. "Security Challenges in Healthcare Cloud Computing: A Systematic Review." Global Journal of Health Science 9, no. 3 (2016): 157.

[8] Sun, Dawei, Guiran Chang, Lina Sun, and Xingwei Wang. "Surveying and analyzing security, privacy and

trust issues in cloud computing environments." Procedia Engineering 15 (2011): 2852–2856.

[9] Khan, Nabeel, and Adil Al-Yasiri. "Identifying cloud security threats to strengthen cloud computing adoption

framework." Procedia Computer Science 94 (2016): 485–490.

[10] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud

computing." Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies 150 (2012).