Authentication of Electronic Health Records Using Visual Cryptography Technique

D.Sasi Preetha[1], Abin Devasia[2], B.Jenis Christina[3], M.Jerrwin Joshua[4], P.Maheswari[5]
[1,2,3,4,5] *Department of Biomedical Engineering, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India.*

Abstract: **In the medical field, Secured transmission and storage of medical images remain a challenge, especially with the growing threat of insider attacks in e-Healthcare systems. These attacks can lead to incorrect health assessments, data misuse, financial losses, and legal or reputational damage for healthcare centers. The reliance on cloud services further increases the risk, making patient records vulnerable and potentially compromising care quality. This highlights the urgent need for effective detection methods. To address this, our study proposes a new framework using watermark extraction and logging detection to identify insider attacks in cloud-based healthcare systems. The approach accurately tracked user activities, distinguishing between legal and illegal access through an audit trail, and demonstrated high precision, recall, and accuracy based on evaluation results.**

Keywords: **Electronic health record, Encryption, Decryption, Watermarking extraction, logging detection, JAVA, JavaScript, MY SQL.**

I. INTRODUCTION

Cloud-assisted mobile health monitoring, which combines mobile communications and cloud computing for decision support, offers improved healthcare quality and reduced costs. However, it raises concerns about client privacy and the intellectual property of service providers, potentially hindering adoption. To address this, outsourced decryption and modified key-private proxy re-encryption techniques shift computation to the cloud without compromising privacy or intellectual property. Our security and performance analysis confirms the effectiveness of this design. Personal Health Records (PHRs), typically stored with third-party cloud providers, also face privacy risks. Encrypting PHRs before outsourcing helps maintain patient control, but challenges remain in ensuring privacy, scalable key management, flexible access, and efficient user revocation for secure, fine-grained data access control.

II. OBJECTIVE

To achieve detailed and scalable data access control for Personal Health Records (PHRs), we employ Attribute-Based Encryption (ABE) to secure each patient's document. Unlike earlier works, our approach supports multiple data owners and classifies users into different security domains, simplifying key management. Multi-authority ABE ensures strong patient confidentiality. The system supports dynamic policy updates, efficient user/attribute revocation, and emergency break-glass access. Analytical and experimental results confirm its security, scalability, and efficiency.

The Health Care System streamlines operations, enhances administration, improves patient care, controls costs, and boosts profitability. It is robust, flexible, user-friendly, and backed by reliable support. Built using database, object-oriented, and networking principles, it uses MySQL for backend data management and JAVA as the object-oriented front-end connected to the database.

The Health Care System is tailored for mid to large-sized hospitals globally, with modules designed to meet specific client needs. Widely accepted in India and abroad, it has received strong client satisfaction. The web-based application is built on a three-tier architecture using modern technologies, with a robust database enhancing usability and scalability. Highly customizable, the system reflects an in-depth study of hospital operations and includes modules like Patient Registration, Medicine, Doctors, Wards, Admin, Store, Appointments, Billing, Records, and Discharge information.

Cloud computing offers an on-demand model for accessing shared computing resources (e.g., servers, storage, applications) with minimal management effort. While it has significant potential across industries like e-business and social networks, it is

still developing, with many offerings lacking open standards, service agreements, and application portability—often locking users into proprietary systems. Developers face challenges in migrating cloud-based applications, and users must trust providers without guaranteed service quality.

This paper introduces a framework for evaluating the value of Cloud Computing compared to traditional IT infrastructure. With more companies adopting cloud services, our goal is to outline economic and technical factors to help determine when cloud outsourcing is practical and when it is not, offering guidance for informed decision-making.

III.EXISTING SYSTEM

The existing framework employs either encryption-only or combined watermarking and encryption approaches. The encryption-only method secures medical records by allowing access only to authorized users with decryption keys, enabling secure access from any location. While this ensures privacy, it cannot detect data modifications by malicious insiders. The combined approach can detect if data has been tampered with, but it cannot identify the insider responsible for the modification.

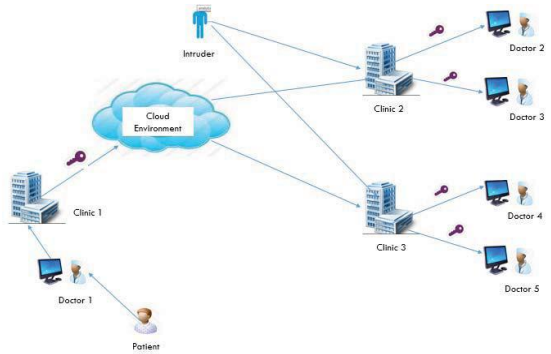

Figure 1.FLOW CHART OF EXISTING METHOD

IV.PROPOSED SYSTEM

We propose a framework capable of detecting any alterations made by insiders, based on the following assumptions:

i. The Cloud and Trusted Third Party are considered secure and trusted by all involved health organizations.

ii. Secure key transmission is not addressed, assuming keys are already securely exchanged through prior models.

iii. Biometric authentication is required for doctors in Clinic2 and Clinic3 to access record R.

iv. The patient's medical record consists of a medical image and disease history.

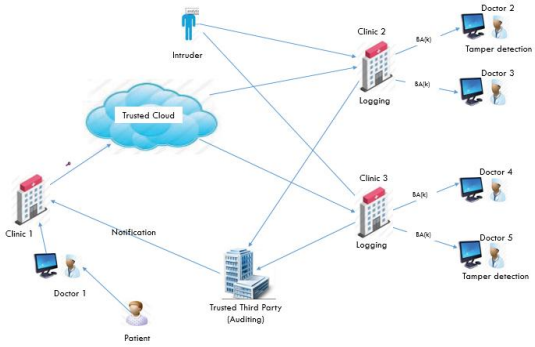

Figure 2. FLOW CHART OF PROPOSED METHOD

The proposed scheme includes five key algorithms:

[1] Setup (K): Initializes the system using a security parameter K, generating the public key (PK) and master key (MK).

[2] Create Attribute Authority (PK, AA): Executed by the central authority (GA) upon an AA request, producing a functional ID (Aid), a set of attributes (Sid), and a secret authority key (SKAid). The Ministry of Health assigns attributes based on the AAs' functions.

[3] Attribute Key Generator (PK, SKAid, Sid): Performed by the Aid domain authority using PK, its secret key (SKAid), and the attribute set (Sid), resulting in attribute secret keys (SKUj) for users.

[4] Encrypt (PK, M, P, PKU): Uses PK, a message (M), an access policy (P), and the public keys (PKU) of attributes in P to produce a ciphertext (CT).

[5] Decrypt (PK, CT, P, SKUj, SKA): Takes PK, the ciphertext (CT), access policy (P), secret user key (SKUj), and secret attribute keys (SKA). If attributes meet the policy, the message is decrypted; otherwise, the output is null.

V. METHODOLOGY

A literature review was conducted on studies from 2014 to 2024 using IEEE Explorer, referenced literature, and various journals. Papers were selected based on their unique approaches, specifically excluding those using watermarking for electronic health record authentication.

Junzuo Lai et al. [1] discussed Attribute-Based Encryption (ABE) with verifiable outsourced decryption, allowing flexible cloud-based access control. A transformation key lets an untrusted cloud convert ABE ciphertexts into simpler forms without revealing content, easing user decryption.

Blaze et al. [2] introduced atomic proxy re-encryption, where a semi-trusted proxy re-encrypts data without accessing the plaintext. Despite some security concerns, updated frameworks improve security and support practical access control in file systems.

Susan Hohenberger and Brent Waters [3] presented a new ABE model reducing ciphertext size and decryption time. A transformation key enables the cloud to generate El Gamal-style ciphertexts while keeping user data private.

A. Koteswaramma and S. Lakshmi Soujanya [4] examined mobile health systems, emphasizing continuous patient connectivity even during communication failures. Their Medical Net design ensures reliable service, fostering user trust.

Justin Brickell et al. [5] proposed a privacy-preserving protocol for evaluating diagnostic programs using branching decision trees. Users only see the output label, maintaining the confidentiality of both the program and the user's data.

Randal Burns et al. [6] developed the Provable Data Possession (PDP) model, enabling clients to verify data storage integrity on untrusted servers. PDP uses probabilistic proofs and minimal metadata, supporting efficient and secure remote storage with low server overhead.

VI. MODULES

1. THE PATIENT
2. HEALTHCARE PROVIDERS
3. TRUSTED AUTHORITY
4. THE E-GOVERNMENT CLOUD-BASED HER
5. PATIENT AND SERVICE PROVIDERS IDENTITY PROOFING
6. THE PROPOSED ACCESS CONTROL
7. DATA DISTRIBUTION
8. ACCESS STRUCTURE OF EHRS
9. WATERMARK

1. THE PATIENT:

The patient is the central entity in the proposed framework. A new patient must request authentication from the trusted authority to receive an ID and access system services. They create a Personal Health Record (PHR), store it on the cloud server, and ensure its security by defining an attribute-based access policy for data encryption before distribution

2. HEALTHCARE PROVIDERS:

Healthcare providers, including physicians, nurses, pharmacists, and other medical staff, offer healthcare services to the community. Each provider needs access to certain parts of patient records for specific tasks. They must obtain an ID from the trusted authority, request a secret key with relevant parameters, and be able to decrypt, modify, and re-encrypt the document using the same key.

3. TRUSTED AUTHORITY:

The trusted authority (TU), like the Ministry of Health, authenticates participants, generates keys for healthcare providers, and publishes necessary cryptographic parameters.

4.THE E-GOVERNMENT CLOUD-BASED EHR:

The e-government cloud-based EHR is central to the framework, part of Saudi Arabia's e-government program. It includes three services: the first service stores encrypted EHRs, accessible only by authenticated healthcare providers through attribute-based access policies. The second service generates access policies, manages keys, and performs necessary computing. The third service hosts a secure web-based portal, accessible 24/7 by stakeholders from any device with an internet connection.

5.PATIENT AND SERVICE PROVIDERS IDENTITY PROOFING:

When applicants access the portal for the first time, that is patients and service providers, they must be registered from the trusted health authority to be able to interact with the system. Through the web portal in the e-government cloud, the applicants can send, update, and receive health information from the cloud's central database with limited access, depending on the end user's privileges.

6.THE PROPOSED ACCESS CONTROL:

The hierarchy starts with the patient uploading their EHR to the cloud with access policies for each service provider. The THA encrypts the EHR with these policies and distributes decryption keys to the relevant providers. A provider can decrypt the file only if the access structure of the encrypted file matches the attributes of their decryption key.

7. DATA DISTRIBUTION:

Due to the fact that the EHR database is very large and contains several users with different access privileges, it is not acceptable for the trusted central authority to encrypt the EHR separately for each user.

It is more efficient to encrypt the EHR only once and distribute the encryption among many attribute authorities (AAs), according to their functionalities.

8.ACCESS STRUCTURE OF EHRS:

The proposed access structure categorizes the users of the EHR into different domains based on their functionalities. There are many different users in the healthcare domain, such as primary care providers, nurses, specialists, pharmacists, medical doctors, and doctors of osteopathic medicine, who focus on family practice, internal medicine, or pediatrics. Each user holds some attributes defined in attribute set. Only those users whose attributes satisfy the access structure defined in the cipher text are able to decrypt the patient's record successfully. The main advantages of using the proposed access structure is achieving lightweight key management when the number of users is large and mitigating and reducing the work load of the GA responsibility to encrypt the EHR, generate decryption keys, and distribute them to the authorized users.

9.WATERMARK:

Watermarked medical images, combined with steganography techniques, offer a promising solution for Electronic Health Record (EHR) authentication. This approach involves embedding a digital watermark within the medical image to identify its origin, authenticity, and integrity. The watermark serves as a digital fingerprint, ensuring that any tampering or alteration of the image can be detected. This technique provides improved security, data integrity, and authentication, making it suitable for applications in telemedicine, electronic health records, and medical research.

VII. SYSTEM SPECIFICATION

HARDWARE SPECIFICATION:

- Processor : Pentium –III
- Speed : 1.1 Ghz
- RAM : 256 MB(min)
- Hard Disk : 20 GB
- Floppy Drive : 1.44 MB
- Keyboard :Standard windows Keyboard
- Mouse :Two or Three button mouse
- Monitor :SVGA

SOFTWARE SPECIFICATION:

- Operating System : Windows 7
- Application Server :Tomcat5.0/6.X
- Front End : Java, JSP
- Script : JavaScript
- Server side Script : Java Server Pages
- Database : MYSQL

VIII. RESULT AND DISCUSSION

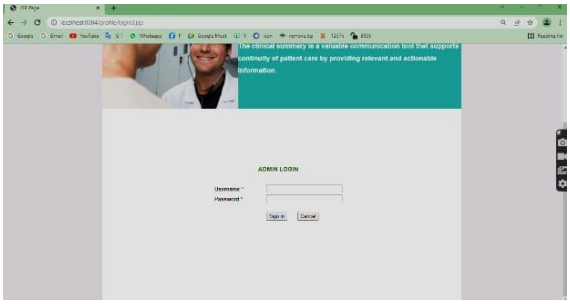

Figure 3.ADMIN LOGIN

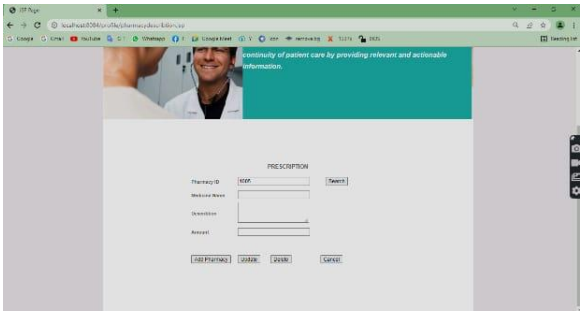

Figure 4.PRESCRIPTION

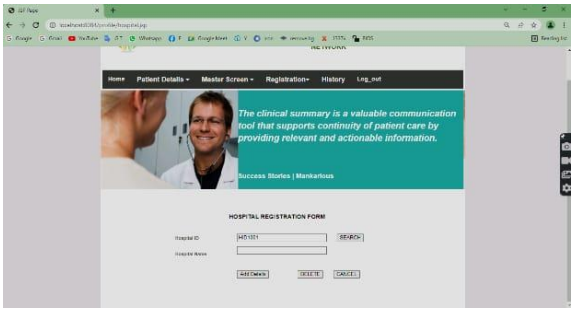

Figure 5.HOSPITAL REGISTRATION FORM

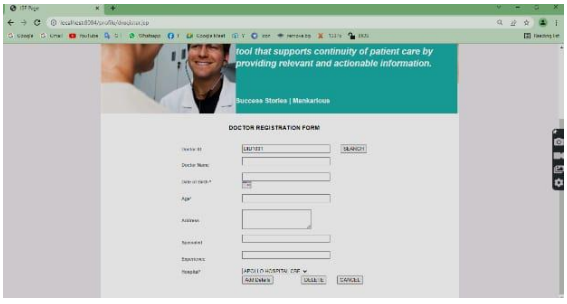

Figure 6.DOCTOR REGISTRATION FORM

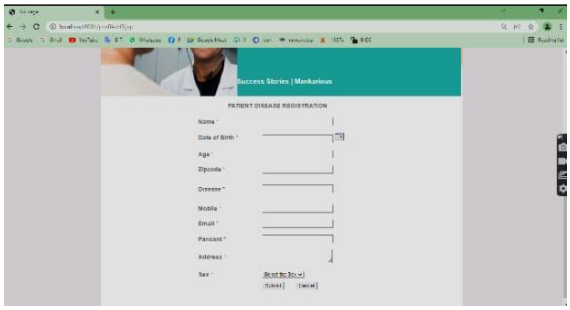

Figure 7.PATIENT DISEASE REGISTRATION

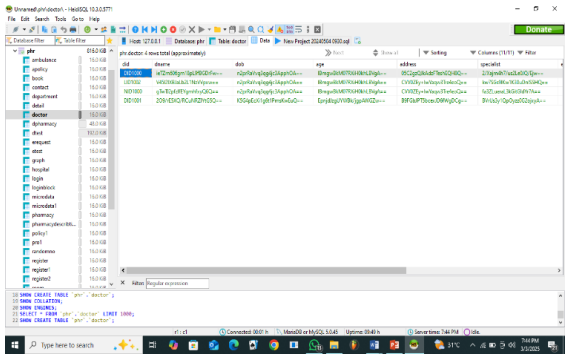

Figure 8.ENCRYPTED MEDICAL DATA

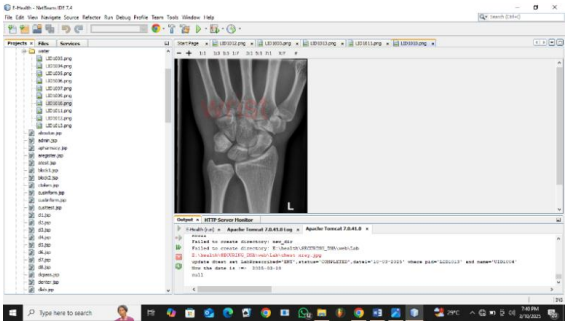

Figure 9.WATERMARKED MEDICAL IMAGE

The proposed framework for detecting insider attacks in cloud-based healthcare systems using watermarking extraction and logging detection techniques demonstrated high precision, recall, and accuracy. The results showed that the framework was effective in detecting and preventing insider attacks, thereby protecting patient health records from unauthorized access and modification. The use of watermarking extraction give an additional layer of authentication and verification, ensuring the genuineness and integrity of medical images. Watermarking also protects the copyright of image owners, prevents unauthorized use or distribution, and safeguards patient data. Furthermore, watermarked images can detect tampering and prevent fraudulent activities. The logging detection techniques provided a robust and reliable means of detecting insider attacks, and the framework's ability to identify the source of the attack was particularly useful in preventing future attacks.

IX. CONCLUSION

In conclusion, the proposed framework for detecting insider attacks in cloud-based healthcare systems using watermarking extraction and logging detection techniques demonstrated high effectiveness in protecting patient health records from unauthorized access and modification. The framework's ability to detect and identify insider attacks, combined with its robust and reliable techniques, make it an excellent solution for securing cloud-based healthcare systems. The results of this study highlight the importance of implementing effective security measures to protect sensitive patient data and demonstrate the potential of the proposed framework to improve the security and privacy of cloud-based healthcare systems.

X. REFERENCE

[1] Blaze, Bleumer, and Strauss, "This is an application called atomic proxy re-encryption", (2012).

[2] Cimato, Stelvio, Ching-Nung Yang, "Visual Cryptography and secret Image Sharing" (2012).

[3] Hohenberger, Susan, Johns Hopkins University, and Brent Waters, "Attribute Based Encryption", (2013).

[4] Johny, Shiji, Anil Antony, "Secure image transmission using visual cryptography scheme without changing the colour of the image" (2013).

[5] Koteswaramma, A., S. Lakshmi Soujanya, "They has discussed about Mobile health system", (2014).

[6] Lai, Junzuo, Robert H. Deng, Chaowen Guan, and Jian Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption", (2013).

[7] Liu, Feng, Wei Qi Yan, "Visual Cryptography for Image processing and security" (2015).

[8] Moataz, Z. Salim, Ali J. Abboud, Remzi Yidrim, "A visual cryptography based watermarking approach for the detection and localization of image forgery" (2015).

[9] Shivdeep, Sudip Ghosh, Prasun Ghosal, Santi Prasad Maity, Hafizur Rahaman, "PEE based reversible watermarking algorithm for authentication and security of medical images" (2014).

[10] Van Tilborg, H.C.A, "Encyclopedia of Cryptography and security" (2005).