Journal of Physico-Chemical Material (JPCM)
Volume 2, Issue 1, Date: 30- June -2025

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.
Email: [1] preethaece@gmail.com, [2] abindevasia345@gmail.com, [3] jenischristina221@gmail.com, [4] jerrwinjoshua@gmail.com, [5] magathilaga@gmail.com
*Corresponding Author

***Abstract*—In the medical field, securely transmitting and storing images has emerged as a challenge. The impact of insider attacks on the e-Healthcare system can result in incorrect assessments of a patient's health records, which have led to a lack of accountability in data usage and significant financial costs due to data breaches in e-healthcare without an effective detection method. Several health centers have encountered legal and reputational repercussions as a result. This situation underscores the need for an effective technique to address this issue, particularly in eHealth systems within cloud environments, as operations currently rely on cloud services. Until such techniques are developed, health records remain vulnerable to attacks, potentially resulting in inadequate patient care due to misinformation, which could ultimately lead to fatalities. This necessity serves as a primary motivation for this study. In this research, we introduced a new framework for detecting insider attacks in Cloud-based Healthcare systems through watermark extraction and logging detection techniques. The approach produced results regarding the activities conducted by users, detailing updates on legal and illegal intrusions into the system via an audit trail. The method demonstrated a high degree of precision, recall, and accuracy, showcasing its excellent performance for implementation based on the evaluations performed at the conclusion of the research.**

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

I. INTRODUCTION

Cloud-assisted mobile health monitoring, which leverages modern mobile communications and cloud computing technologies to provide feedback decision support, has been considered a revolutionary approach for improving the quality of healthcare services while reducing healthcare expenses. Unfortunately, it also poses a considerable risk to both client privacy and the intellectual property of monitoring service providers, which may impede the widespread adoption of health technology. Moreover, the outsourced decryption technique and a newly introduced key private proxy re-encryption have been modified to shift the computational burden of the involved parties to the cloud without compromising client privacy and the intellectual property of service providers. Ultimately, our security and performance analysis demonstrates the effectiveness of our proposed design. Personal health record (PHR) is an emerging patient focused model of health information exchange that is often outsourced for storage at a third party, such as cloud providers. However, substantial privacy concerns have emerged as personal health information could become exposed to those third-party servers and to unauthorized individuals. To guarantee patients' control over access to their own PHRs, it is a promising strategy to encrypt the PHRs before outsourcing them. Nonetheless, challenges such as the risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation remain the most significant obstacles to achieving fine-grained, cryptographically enforced data access control.

II. OBJECTIVE

To attain detailed and scalable data access control for Personal Health Records (PHRs), we utilize Attribute Based Encryption (ABE) methods to secure each patient's PHR document. Unlike earlier studies on secure data outsourcing, we concentrate on a scenario with multiple data owners and categorize users within the PHR system into various security domains, significantly simplifying key management for both owners and users. A high level of patient confidentiality is ensured concurrently through the use of multi-authority ABE. Our system also facilitates the dynamic adjustment of access policies or file attributes, accommodates efficient on-demand user/attribute revocation, and allows break-glass access in emergency situations. Comprehensive analytical and experimental findings are provided, which demonstrate the security, scalability, and efficiency of our proposed approach.

The Health Care System offers streamlined operations, improved administration and oversight, enhanced patient care, rigorous cost management, and increased profitability. It is robust, adaptable, and user-friendly, designed and developed to yield tangible benefits for hospitals. Crucially, it is supported by reliable and trustworthy assistance.

The initiative 'Health Care System' is grounded in database, object-oriented, and networking methods. Given that there are several areas where we maintain records in a database, we utilize MY SQL software, regarded as one of the best and simplest platforms for managing our information. This project employs JAVA as the front-end software, which is based on Object-Oriented Programming and connects with MY SQL.

Received: 28-03-2025
Revised: 18-06-2025
Published: 30-06-2025

The Health Care System is custom-designed to address the specific needs of mid to large-sized hospitals worldwide. All essential modules and features have been specifically developed to align with your requirements. This package has gained wide acceptance among clients in India and abroad. Not only that, but clients are also highly satisfied and express their appreciation. The entire application is web-based and developed on a three-tier architecture using the latest technologies. The robust database of the application enhances user-friendliness and scalability.

The package is exceptionally customizable and can be adjusted according to our clients' needs and specifications. An extensive study of hospital functionalities and their unique requirements has shaped it remarkably in both technical and usability aspects. It encompasses all necessary modules, including Patient Registration, Medicine details, Doctor, Wards, Admin, Store, Patient appointments, bill payments, record modifications, discharge information, etc.

Cloud computing represents a contemporary model for providing convenient, on-demand network access to a shared pool of configurable computing resources (e. g. , networks, servers, storage, applications, and services) that can be swiftly provisioned and released with minimal management effort or interaction with service providers. Currently, clouds are predominantly utilized in commercial environments and emphasize the on-demand provision of IT infrastructure. Cloud computing has the potential to significantly impact various fields, including innovations, virtual worlds, ebusiness, social networks, and search engines. However, at this stage, it remains in its infancy, with ongoing consistent experimentation expected. Cloud computing solutions are presently implemented in environments where they were developed without addressing a unified programming model, open standard interfaces, sufficient service level agreements, or application portability. Overlooking these issues, current Cloud computing offerings compel users to become trapped in locked, proprietary systems. Developers striving to Cloudify their applications find it challenging to transfer them elsewhere. Additionally, users entrust commercial providers with applications and data without a negotiable quality of service agreement.

The primary aim of our paper is to introduce a fundamental framework for assessing value and determining benefits from Cloud Computing as an alternative to traditional IT infrastructure, such as privately owned and managed IT hardware. Our endeavor is driven by the emergence of Cloud Computing providers and the inquiry of when it is practical for a business to utilize hardware resources in the Cloud. An increasing number of companies have already integrated Cloud Computing services into their IT infrastructure. However, no guidelines exist to indicate when outsourcing to the Cloud is advisable and in which scenarios it may not be reasonable to proceed. Through our work, we aspire to provide an overview of the economic and technical factors that a valuation approach to Cloud Computing needs to consider.

III. EXISTING SYSTEM

The existing framework that has been employed utilizes either encryption only or watermarking and encryption Approaches. The encryption only approach ensured security and privacy of medical records. This approach combines a list of authorized users which is used for reading and encrypting the records. The encrypted data can then be decrypted by an authorized user who uses a key. The authorized user can access these data which have been sent to the cloud environment irrespective of the location of the health center that the data is sent from. The medium was secured using encryption but malicious insiders could pose an attack on the data by modifying it without being detected. The watermarking and encryption approach was able to detect that a modification have been done by a malicious insider but the insider who performed the action was not detected

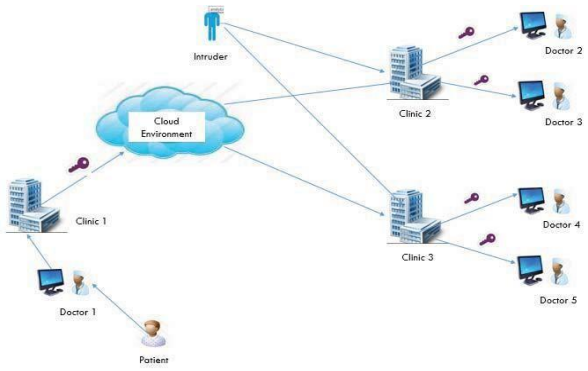

Fig. 1. Flow chart of the existing method

IV. PROPOSED SYSTEM

We hereby propose a framework that has the essential features for detecting any alteration by an insider. The following assumptions hereby exist in our proposed model:

i. Trusted Cloud and Trusted Third Party are assumed security entities believed to be granted trust by all the Involving health organizations.

ii. The secure transmission of keys is not put into consideration based on key exchange policies with the Assumption that every key have been catered for by the prior model and transmitted securely.

iii. A biometric authentication approach is used to access the record R by any doctor in Clinic2 and Clinic3.

iv. We will be using a medical image and disease history as the medical record of patient.

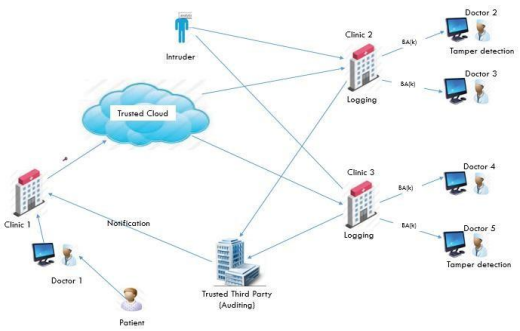

Fig. 2. Flow chart of proposed method

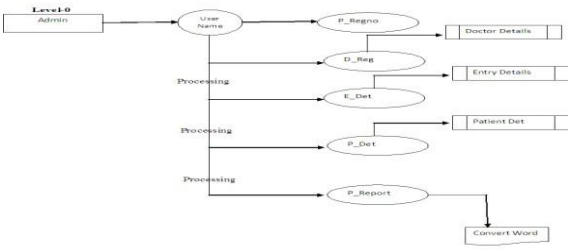

Fig. 3. Data flow diagram

The suggested scheme comprises the following five algorithms: [1] Setup (K). This algorithm establishes the system by taking a security parameter, K, as an input. It produces the public key (PK) and the master key (MK) as outputs.

[2] Create Attribute Authority (PK, AA). The GA (central authority) executes this algorithm with the AA request as input. It generates a functional identifier, Aid, for the AA along with a collection of attributes, Sid, and a secret authority key, SKAid. The Ministry of Health classifies the AAs based on their functions and subsequently allocates attributes for the users of these functions.

[3] Attribute Key Generator (PK, SKAid, Sid). This algorithm is carried out by the Aid domain authority. It requires the PK and the domain authority's secret key, SKAid, along with the set of attributes, Sid, as inputs. It produces the attribute secret keys for the user SKUj as outputs.

[4] Encrypt (PK, M, P, PKU). The encrypt algorithm takes the PK, a message (M), an access policy (P), and the collection of public user keys (PKUs) corresponding to all the attributes in P as inputs. It outputs the cipher text message CT. [5] Decrypt (PK, CT, P, SKUj , SKA). The decrypt algorithm takes the PK, a cipher text message CT, the identical access P used during encryption, the secret user key, SKUj, and the collection of secret attribute keys, SKA as inputs. The CT message will be decrypted if the attributes are adequate to satisfy P; otherwise the output will be null.

V. 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

VI. METHODOLOGY

A literature review was conducted, focusing on studies published between 2014 and 2024. The searching technique involved utilizing the IEEE Explorer, the referenced literature in the included articles, and a range of journals. The chosen papers were selected based on the differentiation they provided, explicitly focusing on methods that had not applied the watermarking technique in the authentication of electronic health records. Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng [1] "Attribute-Based Encryption With Verifiable Outsourced Decryption" discussed that Attribute-based encryption (ABE) constitutes a public-key based done-to-many encryption approach that enables users to encrypt and decrypt information according to user attributes. A notable application of ABE is its adaptable access control of encrypted information stored in the cloud, utilizing access policies and attributes attributed to private keys and cipher texts. ABE systems featuring outsourced decryption significantly reduce the decryption burden for users. In this configuration, a user gives an untrusted server, like a cloud service provider, a transformation key permitting the cloud to convert any ABE cipher text that meets that user's attributes or access policy into a simplified cipher text, incurring only minimal computational expenditure for the user to retrieve the plaintext from the modified cipher text. The security of an ABE system with outsourced decryption ensures that a malicious entity (including an untrustworthy cloud) will not uncover any details about the encrypted communication; however, it does confirm the accuracy of the transformation executed by the cloud (2013). Blaze, Bleumer, and Strauss [2] focused on an application termed "atomic proxy re-encryption," in which a semi-trusted proxy changes one cipher text for Alice into another cipher text for Bob without accessing the original plaintext. We predict that rapid and secure re-encryption will become progressively favored as a technique for managing encrypted file systems. Despite its computability, the widespread acceptance of BBS reencryption has faced significant security challenges. Building on recent research by Ivan and Dodis, they present new reencryption frameworks that achieve a fortified standard of security, demonstrating the practicality of proxy re-encryption as a method for enhancing access control within the SFS read-only file system. Experimental performance evaluations of our file system showcase that proxy re-encryption can function efficiently in real-world applications (2012). Susan Hohen berger, Johns Hopkins University, and Brent Waters [3] examined "Attribute Based Encryption," describing that attribute-based encryption (ABE) represents a fresh perspective toward public key encryption, allowing users to encrypt and decrypt communications based on user attributes. For instance, a user may create a cipher text that can only be decrypted by other users possessing attributes that fulfill ("Faculty" OR ("PhD student" AND "Qualification Completed")). Due to its expressive capabilities, ABE is currently being evaluated for numerous cloud storage and computing applications. Nonetheless, a significant efficiency drawback of ABE is that both the size of the cipher text and the decryption time increase with the complexity of the access policy. In this study, we introduce a new framework for ABE that

substantially reduces this burden for users. With ABE cipher texts stored in the cloud, it illustrates a method by which a user can provide the cloud with a single transformation key that enables the cloud to convert any ABE cipher text fulfilling that user's attributes into a (constantsize) El Gamal-style cipher text, while preventing the cloud from reading any part of the user's messages (2013). A. Koteswaramma, S. Lakshmi Soujanya [4] discussed the mobile health system, where a mobile healthcare system consists of a network that includes numerous components, from patients to their healthcare providers. It is crucial that the patient remains continuously connected, even if one of the communication components fails. The design of the Medical Net system demonstrates how it smoothly addresses connectivity challenges between patients and their mobile devices, among healthcare meters and mobile phones, and connecting mobile phones with web server components. The primary objective behind our design strategies is to consistently deliver a superior level of service to the patient in the face of communication disruptions, improving both acceptance and trust in the system by patients (2014). Justin Brickell, Donald E. Porter, Vitaly Shmatikov, and Emmett Witchel [5] presented a privacy-preserving system and introduced an efficient protocol for the privacy-preserving evaluation of diagnostic programs, represented as binary decision trees or branching programs. This protocol employs a branching diagnostic program with classification labels at the leaves that is applied to the user's attribute vector. The user learns solely the label designated by the program for his vector, while the diagnostic program itself remains confidential. The program's owner does not receive any information. Our construction is notably more efficient than those obtained through direct application of generic secure multi-party computation techniques (2013). Randal Burns, Giuseppe Ateniese, Reza Curtmola, and Dawn Song [6] formalized a model for Provable Possession (PDP) which enables a client, having retained data with an untrustworthy server, to verify that the server possesses the original data without retrieving it. The model produces probabilistic proofs of possession by randomly sampling sets of blocks from the server, generating a minimal amount of metadata required to validate the proof. The challenge-response protocol transmits a small, constant amount of data that minimizes network data verification and supports large data sets in wide-ranging communications. Therefore, the PDP model is effective for remote distributed storage systems. It provides two solutions, revealing provably-secure PDP schemes that outperform previous methods, even in comparison to those achieving weaker guarantees. Notably, the server's overhead remains low (or even constant), rather than linear in relation to the data size (2014).

A. The patient:

The patient is the main entity in our proposed framework. The patient has the following main tasks: A new patient must apply for an authentication request to the trusted authority to get his or her identification number (ID), and then he or she will be able to use the system services. Creates the patient history record (PHR) and stores it at the cloud server.

Ensures the PHR is fully secured and protected by defining an (attribute-based) access policy that can be used for encrypting the data before it is distributed.

B. Healthcare providers:

Healthcare providers are individuals who provide healthcare services of all kinds in an organized manner to all members of a community. The healthcare providers could include the following members: health practitioners and specialists, physicians, nurses, pharmacists, surgeons, medical technicians, laboratory workers, and other employees. Each of these members must have access to some part of the patient records for specific purposes. Each healthcare provider must complete the following tasks: Apply for an identification number (ID) from the trusted authority to be able to access specific parts of the patient's record. Apply a request for the secret key attached with the appropriate parameters. Be able to decrypt, modify, and encrypt the same document with the same key.

C. Trusted authority:

The trusted authority (TU), such as the Ministry of Health or any government sector, is responsible for the following functions: Authenticate all participants who interact with the system. Generate keys for healthcare providers and publish public parameters required by cryptographic operations.

D. The e-government cloud-based EHR:

The e-government cloud-based EHR is the backbone of our proposed framework. In the Kingdom of Saudi Arabia, the e-government program has been established, and one of its initiatives and products is government cloud computing. The proposed e-government cloud-based EHR consists of the following cloud services. The first service consists of two fundamental parts. Data repository and computing resources. The first service is responsible for storing the encrypted EHRs that are accessible only by the authenticated healthcare providers through an access policy based on healthcare provider attributes. The second service is responsible for generating the access policies, providing efficient keys management, and performing other required computing processes. The third service is hosting the web-based portal. The developed web-based portal should be a secure online website that can be accessed by the stockholders from anywhere, with 24-hour a day access, through Internet connection, and can be accessed by any device.

E. 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.

F. The proposed access control:

The hierarchy begins with the patient uploading his or her EHR to the cloud associated with the access policies for every service provider, according to their domains and types. The THA encrypts the patient's EHR, attached with the

defined policies, and distributes different decryption keys to the corresponding service providers. When the healthcare service provider retrieves an encrypted EHR, the service provider can decrypt the file if, and only if, there is a match between the access structure of the encrypted file and the attributes associated with his or her decryption key.

G. 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.

H. 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.

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

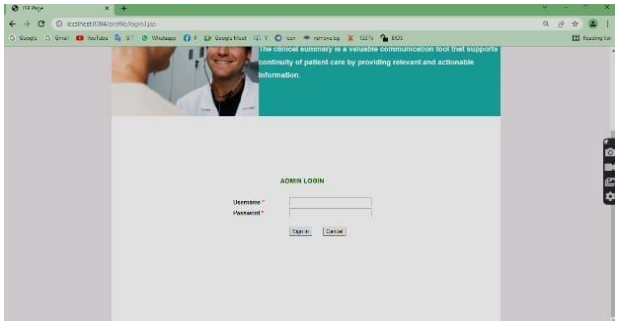

Fig. 4. Admin login

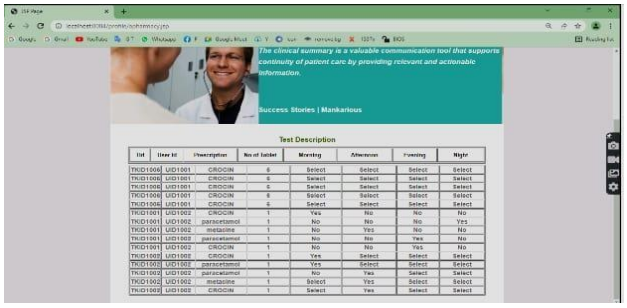

Fig. 5. Test description

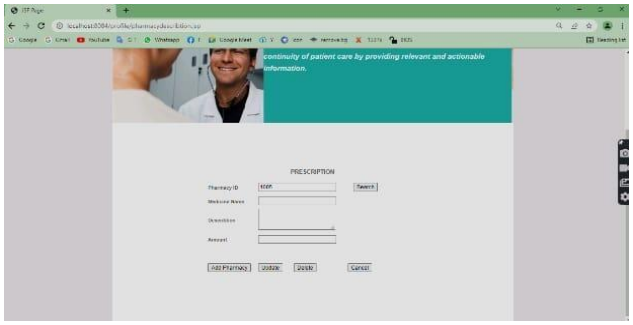

Fig. 6. Prescription

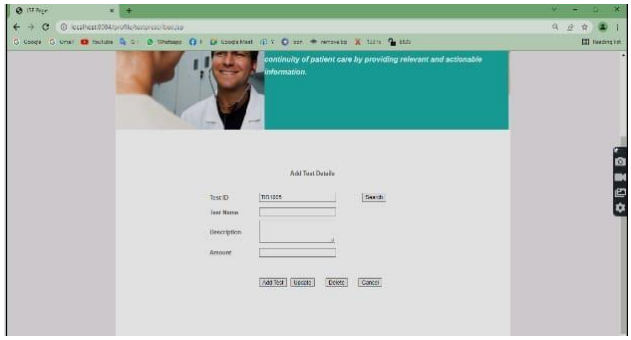

Fig. 7. Add text details

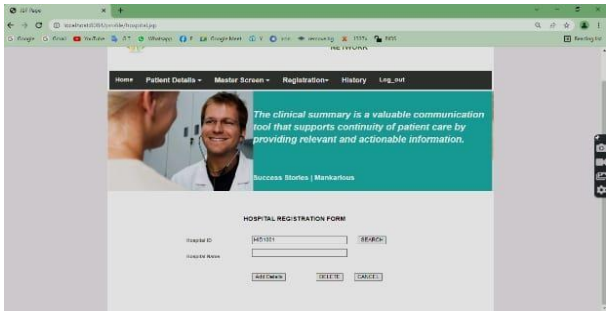

Fig. 8. Hospital registration form

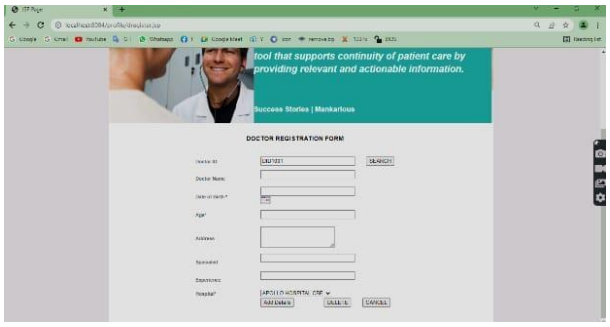

Fig. 9. Doctor registration form

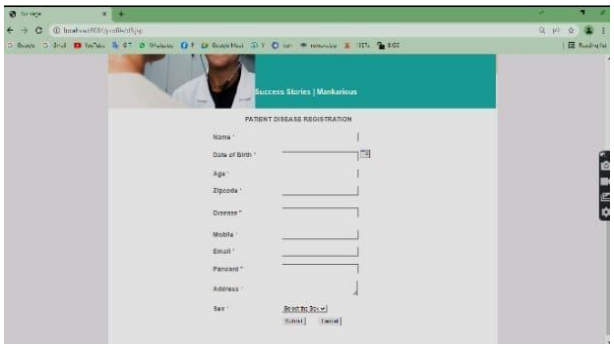

Fig. 10. Patient disease registration

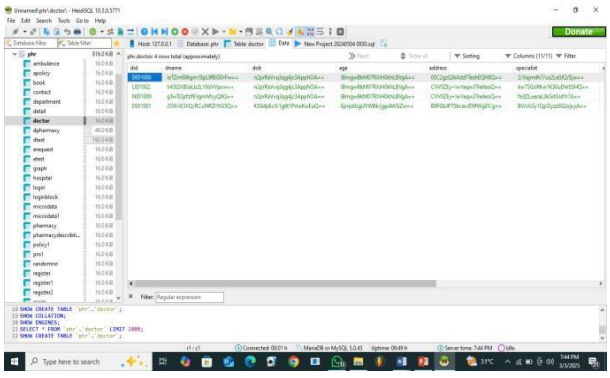

Fig. 10. Encrypted medical data

Fig. 11. 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.

REFERENCES

[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).