Access Control With Anonymous Authentication for Personal Health Record

***Devaraju H B, ** Dr. Akshath M.J**
**P G Student, USN – 4MH22SCS01, **Associate Professor*
Dept of CSE, MITM, Mysore

[1]*Received: 09 April 2024; Accepted: 28 June 2024; Published: 12 July 2024*

ABSTRACT

A smart healthcare system that provides mutual benefits to both patients and physicians is the Personal Health Record (PHR) system. Typically, a semi-trusted cloud provider oversees the management and storage of PHRs on cloud infrastructure. However, personal health information remains vulnerable to unauthorized access by external entities and semi-trusted parties. This research proposes a patient-centric PHR sharing architecture designed to enhance patient privacy and ensure patients' autonomy over their PHRs. The proposed system addresses the core issue of secure data hosting and implements fine-grained access control to PHRs by employing multi-authority attribute-based encryption (MA-ABE) prior to outsourcing. Furthermore, it is recommended to implement anonymous authentication mechanisms between users and the cloud to ensure data integrity while preserving user anonymity. The proposed authentication scheme utilizes a novel online and offline attribute-based signature (ABS) to enhance security. This approach not only bolsters patient control over their PHRs but also mitigates the risk of collusion attacks and ensures the integrity of encrypted PHRs during the sharing process. The adoption of online, offline, or outsourced decryption methods reduces computational overhead and enhances system efficiency.

Keywords: *Personal Health Record (PHR); Multiauthority Attribute-Based Encryption (MA-ABE); Cloud Computing; Semi-Trusted Cloud Provider*

INTRODUCTION

The Personal Health Record (PHR) system, an emergent technology, has played a pivotal role in facilitating data exchange in recent years. PHR enables patients and healthcare providers to access medical records online, providing flexibility to retrieve information anytime and from anywhere. However, the implementation of PHR systems also raises concerns, particularly regarding privacy breaches during data sharing. To address these challenges and enhance patient privacy and control, a fine-grained access control mechanism based on Attribute-Based Encryption (ABE) has been proposed, garnering significant attention in the field. ABE generates private keys or ciphertext using specific attributes, allowing access to PHRs only for users whose attribute sets satisfy the predefined access policies. The Personal Health Record (PHR) system, an emergent technology, has played a pivotal role in facilitating data exchange in recent years. PHR enables patients and healthcare providers to access medical records online, providing flexibility to retrieve information anytime and from anywhere.

However, the implementation of PHR systems also raises concerns, particularly regarding privacy breaches during data sharing. To address these challenges and enhance patient privacy and control, a fine-grained access control mechanism based on Attribute-Based Encryption (ABE) has been proposed, garnering significant attention in the field. ABE generates private keys or ciphertext using specific attributes, allowing access to PHRs only for users whose attribute sets satisfy the predefined access policies.

[1] *How to cite the article:* Devaraju H.B., Akshath M.J. (July, 2024); Access Control With Anonymous Authentication for Personal Health Record; *International Journal of Advances in Engineering Research*, July 2024, Vol 28, Issue 1, 11-22

The utilization of a Personal Health Record (PHR) system facilitates data exchange and storage, yet it presents considerable risks of privacy leakage, particularly when sensitive user information stored on cloud platforms is accessed by unauthorized individuals. This scenario compromises the direct control patients have over their PHRs. As a result, cloud-based PHR systems are more susceptible to both internal and external threats compared to traditional paper-based PHRs. Thus, it is imperative to implement a secure and private PHR system with fine-grained access control mechanisms to safeguard sensitive data and maintain patient autonomy.

Figure 1: Access control Authentication

In previous methodologies, users are required to submit their identities or attribute sets to a cloud server in order to receive the corresponding ciphertext. This procedure inherently risks exposing sensitive information, as the cloud server gains access to users' confidential data. Moreover, the cloud server possesses the potential to manipulate the initial ciphertext, either by substituting it with an alternative transformation or by returning a forged response, symbolized as a terminator ⊥. To address these vulnerabilities, we propose a novel framework that synergistically integrates attribute-based encryption (ABE) with attribute-based signatures (ABS). This hybrid approach seeks to optimize the balance between safeguarding users' privacy and ensuring data security.

Our proposed framework includes an anonymous authentication protocol between the cloud and the user, which ensures the integrity of the data stored in the cloud, thereby preventing data forgery. Furthermore, the anonymity provided by the protocol protects users' identities during the authentication process, thereby preserving user privacy. To facilitate lightweight computational demands, we employ an offline-online technique in conjunction with outsourcing decryption operations. This combination aids in the authentication process and allows for partial decryption, thereby enhancing the efficiency and security of the system.

LITERATURE SURVEY

To securely share outsourced data across public cloud servers, this research, led by Sana Belguith, proposes the InsPAbAC framework, which integrates Attribute-Based Encryption (ABE) and Attribute-Based Signing (ABS) techniques. The proposed architecture offers several advantages. Firstly, it facilitates the implementation of encrypted access control at the data owner's end, allowing for the specification of highly expressive access control policies. This approach enhances security and ensures that only authorized users can access the data, thereby providing a robust mechanism for data protection and privacy preservation.

Secondly, InsPAbAC safeguards users' privacy by concealing users' personal information through an anonymous authentication method derived from a privacy-preserving attribute-based signature scheme. This ensures that sensitive identity details remain protected even during authentication processes.

Furthermore, Fog Computing, as introduced by Daweili, extends the Cloud Computing paradigm to the network's edge, providing computation, storage, applications, and network services between Internet of Things (IoT) devices and cloud servers. This paradigm shift necessitates a focus on information security, while also offering enhanced security features with low latency. Additionally, Fog Computing supports extensive geographical distribution and high flexibility, owing to its large number of distributed nodes. These characteristics make Fog Computing an ideal solution for scenarios requiring real-time processing and data management in distributed environments.

We propose a novel cryptographic primitive, **CCA2** Secure Publicly-Verifiable Revocable Large-Universe Multi-Authority Attribute-Based Encryption (CCA2-PV-R-LU-MA-ABE)**,** designed to provide a flexible and fine-grained access control mechanism in Fog Computing environments. In this primitive, Fog end nodes generate private keys sourced from multiple authorities, which can be distinguished based on their roles or geographical locations. The attributes in this system can be represented as arbitrary strings within a large universe, thereby accommodating a diverse array of requirements in practical Fog Computing applications. This design ensures secure and efficient management of access permissions, with the added capability of public verification and revocability, thereby enhancing the overall security and functionality of the system.

This primitive ensures that only valid ciphertexts are retained or transmitted and facilitates public verification to confirm the integrity of the ciphertext. Our CCA2-PV-RLU-MA-ABE technique is a tangible implementation, leveraging the underlying cryptographic outmoded and the unique attributes of Fog Computing. We delineate the security model of this primitive, through which offers a significantly higher level of security compared to ciphertext-Policy Attribute-Based Encryption (CPA-secure) method. Furthermore, we conduct a comparative analysis of the proposed technique's efficiency against the current CPA-secure methodology through both theoretical evaluations and empirical experimentation. The findings demonstrate that additional computational overhead incurred to enhance security is justified by the increased protection and functionality provided. In prior systems, users were required to submit their identities or attribute sets to the cloud server in exchange for ciphertext, thereby exposing their private information to potential misuse. Our approach mitigates this vulnerability by ensuring that sensitive user data is protected and not disclosed to the cloud.

The cloud has the potential to compromise data integrity by replying with a forged transformation, thereby altering or tampering with original ciphertext. It may even deceive users by masquerading as a legitimate terminator. Our proposal addresses these vulnerabilities by integrating Attribute-Based Encryption (ABE) and Attribute-Based Signatures (ABS) into a cohesive system that optimizes the balance between data security and user privacy protection. To further reinforce data integrity and prevent tampering, we advocate for the use of anonymous authentication between users and the cloud. The anonymity provided by the protocol ensures that users' identities remain confidential throughout the authentication process, thereby safeguarding their privacy. Additionally, we implement an offline-online approach, outsourcing partial decryption and authentication processes to achieve lightweight computation. This strategy reduces the computational burden on end users, enhancing the efficiency and scalability of the system while maintaining robust security measures.

Health care management systems play a pivotal role in preserving records from destruction, as these records provide critical evidence of ownership, legal status, received accounts, and specific obligations from public or private entities. Whether in printed or electronic form, these documents are indispensable for maintaining business continuity during emergencies and facilitating the resumption of operations thereafter. According to McDougall [1], approximately 1,500 Australian enterprises are destroyed by fire annually, underscoring the importance of robust record preservation strategies.

The safeguarding of such records is not only a moral and legal obligation but also a practical necessity to ensure the uninterrupted provision of healthcare services and the protection of organizational and patient interests. In the three years following a fire, nearly 70% of enterprises that experienced the loss of computer programs and paper documents were forced out of business. Similarly, the terrorist attacks on September 11, 2001, led to the destruction of numerous critical records in the United States. During such catastrophic events, electronic records, unlike paper documents, are often more amenable to preservation through the maintenance of backups stored at geographically disparate locations. This practice ensures continuity of information and operational resilience in the face of disaster, highlighting the crucial role of robust backup strategies in mitigating the impact of record loss. Computer based the patient record serves as the principal repository of information regarding an individual's medical care. It influences nearly every stakeholder involved in the provision, receipt, or reimbursement of healthcare services. Remarkably, despite the significant technological advancements in healthcare over the past several decades, the contemporary patient record remains strikingly analogous to its counterpart from fifty years ago. This stagnation in the evolution of patient records exacerbates the already strained healthcare system, particularly as the informational demands of practitioners continue to escalate.

The static nature of patient records is thus compounding existing challenges, highlighting an urgent need for modernization to meet the evolving requirements of contemporary medical practice. The intricate machinery of our healthcare system has become increasingly incapable of assimilating and understanding the diverse experiences of patients.

Healthcare executives, physicians, and payers frequently lack a unified perspective on the patient's comprehensive health journey. Consequently, the healthcare system has devolved into a disordered and unstable entity, in urgent need of a central coordination mechanism to navigate the complexities of contemporary medical practice. The current system is marked by inefficiencies and suboptimal decision-making processes. Enhancing patient records could significantly transform the healthcare system. In a 1991 report on computerized medical records, the General Accounting Office (GAO) identified three principal methods through which improved patient record management could enhance healthcare outcomes.

METHODOLOGY

System Architecture and Components: The proposed system for Access Control with Anonymous Authentication is comprised of the following key components:
Operating System: The application will be deployed on machines running Windows 7 and above.
Programming Language: The server-side logic and processing will be implemented using Java, specifically leveraging Servlets for handling HTTP requests and responses. Storage: MySQL will serve as the relational database management system (RDBMS) to store user data, access control policies, and system logs. Frontend Technologies: The user interface will be developed using HTML,CSS, and JavaScript, providing an interactive and responsive experience.

Anonymous Authentication Protocol: To protect user privacy, an anonymous authentication protocol will be employed. This protocol ensures that the user's identity is not revealed during the authentication process while still verifying the user's eligibility to access certain resources.
Attribute-Based Encryption (ABE): Users will be authenticated based on their attributes rather than their identities. ABE allows encryption based on user attributes, such that only users with matching attributes can decrypt the data.
Attribute-Based Signature (ABS): To ensure data integrity and non-repudiation, users will digitally sign their requests using ABS. This mechanism binds the signature to a set of attributes without revealing the user's identity.

Data Storage and Access Control: MySQL Database: The database schema will include tables for storing user attributes, encrypted data, access policies, and transaction logs. The database will enforce strict access control policies to ensure that only authorized entities can access or modify sensitive information.
Policy Definition and Enforcement: Access control policies will be defined based on user attributes and roles. The system will dynamically evaluate these policies during each access request, ensuring that only authorized users can access specific resources.

Offline-Online Technique for Efficiency: To reduce the computational overhead on the client side, an offline-online technique will be implemented. This approach involves two phases:
Offline Phase: Certain computationally intensive operations, such as the setup and generation of cryptographic keys, will be pre-computed and stored securely. Online Phase: During the actual authentication and data access, the system will use the pre-computed values to perform lightweight operations, minimizing the computational burden on the

client device. Outsourced Decryption Operations For efficient data retrieval, decryption operations will be partially outsourced to the cloud server. The cloud will perform initial decryption steps, while the final decryption key, which resides with the user, will be used to fully decrypt the data. This ensures that the cloud cannot access the plaintext data, thus preserving data confidentiality.

System Security and Privacy Considerations Data Integrity: ABS ensures that data sent and received cannot be tampered with. Any unauthorized modification can be detected, maintaining data integrity. User Anonymity: The authentication protocol guarantees that users' identities remain anonymous throughout the process, protecting their privacy. Secure Communication: All data transmissions To mitigate the risk of man-in-the-middle attacks and eavesdropping, Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption protocols will be employed to secure communications between the client and server.

Implementation and Testing Development Environment: The system will be developed using an integrated development environment (IDE) like Eclipse, with Java as the primary programming language. Testing and Validation: The system will undergo a series of evaluations, including user acceptability testing**,** integration testing**, and** unit testing**.** User acceptability testing will assess the system's functionality and usability from the perspective of end-users. Integration testing will examine the interaction between different system components to ensure they work cohesively. Unit testing will focus on verifying the correctness of individual components or modules of the system. will focus on ensuring the correctness of access control policies, the security of the anonymous authentication protocol, and the overall robustness of the system.

WORKFLOW DIAGRAM

Illustrating the process of Access Control with Anonymous Authentication. The diagram outlines the key steps, from the client initiating a request to final decision on data access. The arrows indicate the flow of information and decision-making through the system.

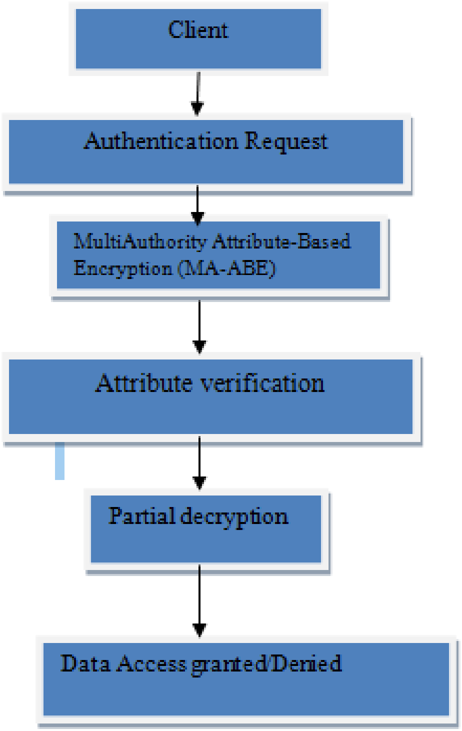

Client
Authentication Request
MultiAuthority Attribute-Based Encryption (MA-ABE)
Attribute verification
Partial decryption
Data Access granted/Denied

Figure 2: Access Control with Anonymous Authentication

Client: The client is the entity that wants to access a resource. This could be a user or a system requesting access.

Authentication Request: The client sends an authentication request to the access control system. This request typically includes necessary details for verifying the client’s attributes.

Multi-Authority Attribute-Based Encryption (MA-ABE):MA-ABE is a cryptographic method used to enforce access control policies based on user attributes. Multiple authorities are involved in this system, each managing a different set of attributes.

Attribute Verification: The access control system verifies the attributes provided by the client against the attributes defined by the authorities. This step ensures that the client meets the criteria set by the access control policies.

Partial Decryption: If the attributes are verified successfully, the system performs partial decryption of the encrypted data. This decryption is based on the attributes and the policy that governs access.

Data Access Granted/Deny:

Access Granted: If the partial decryption is successful and the client meets the access control policy requirements, the system grants access to the requested data. Access Denied: If the client does not meet the criteria, or if the decryption fails, the system denies access to the data.

RESULTS

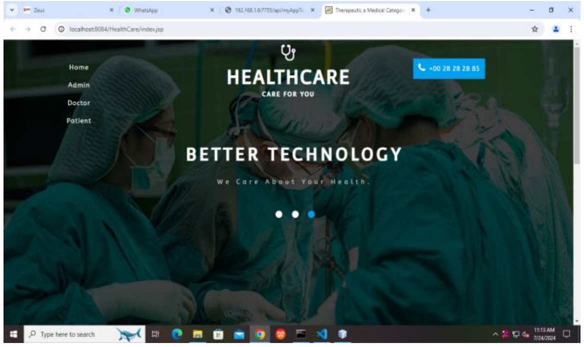


Figure 3: Homepage

..

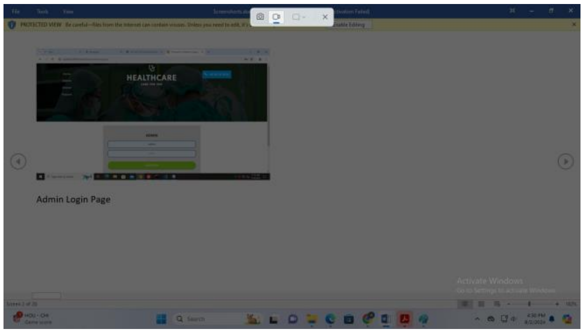


Figure 4: Admin Login page

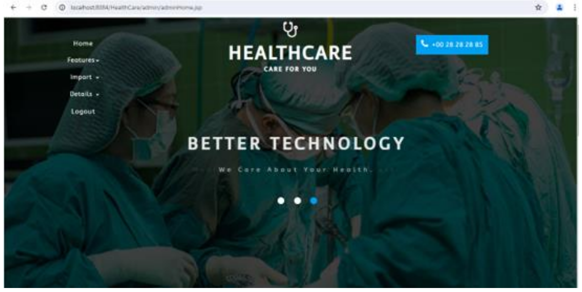
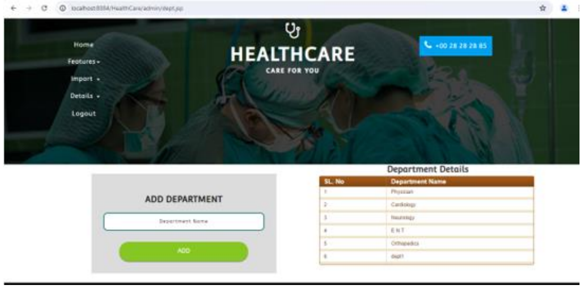


Figure 5: Admin Home page



Department Details

SL. No	Department Name
1	Physician
2	Cardiology
3	Neurology
4	E N T
5	Orthopedics
6	dept1

Figure 6: Add Department

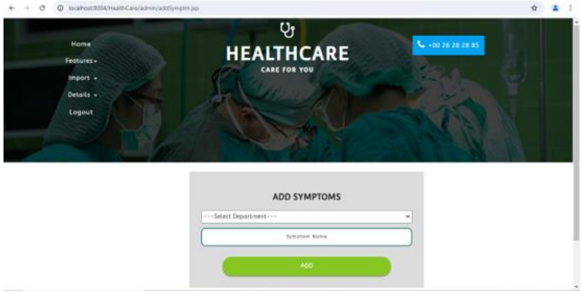
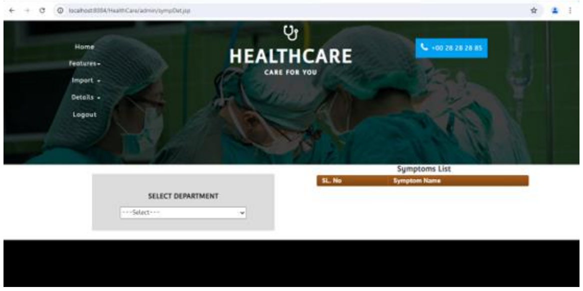


Figure 7: Add Symptoms



Symptoms List

SL. No	Symptom Name

Figure 8: Add Symptoms details

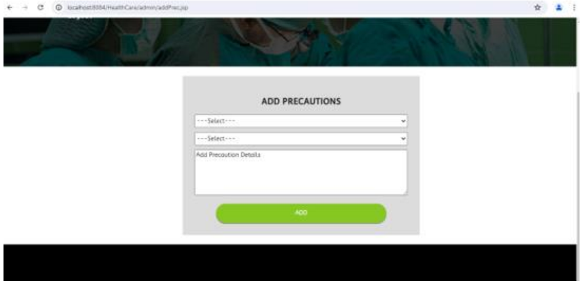


Figure 9: Add precautions

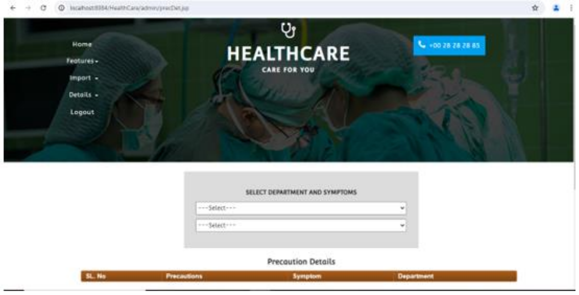


Figure 10: Precaution details Add

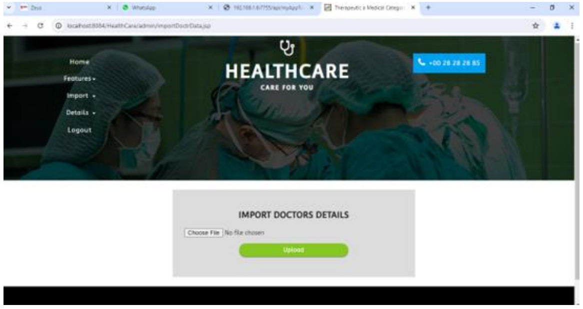


Figure 11: Import doctor data

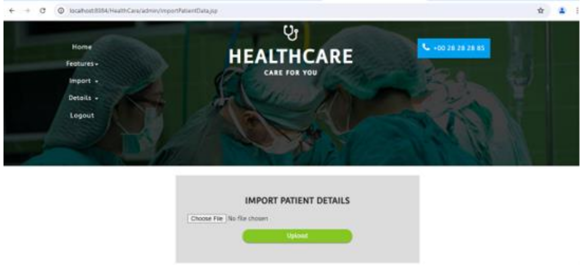
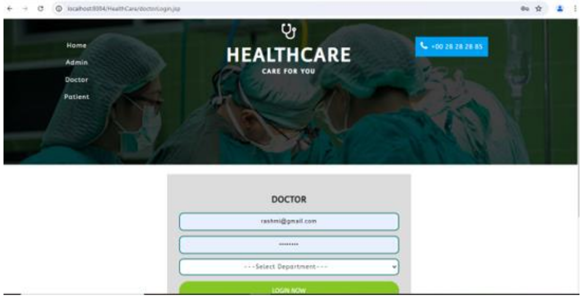


Figure 12: Import patient details



DOCTOR

rashmi@gmail.com

••••••••

---Select Department---

Figure 13: Doctor login Page

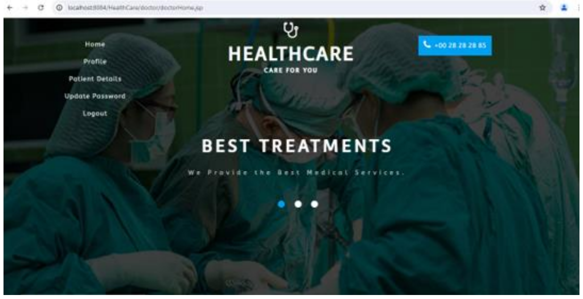
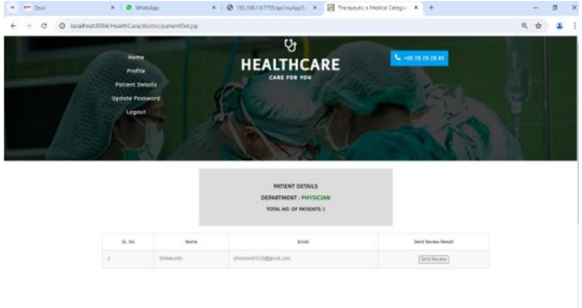


Figure 14: Doctor Home Page

Figure 15: Doctor Profile



PATIENT DETAILS

DEPARTMENT : PHYSICIAN

TOTAL NO. OF PATIENTS: 1

SL. No	Name	Email	Send Review Result
1	Shreekanth	shreekanth1210@gmail.com	Send Review

Figure 16: Patient details

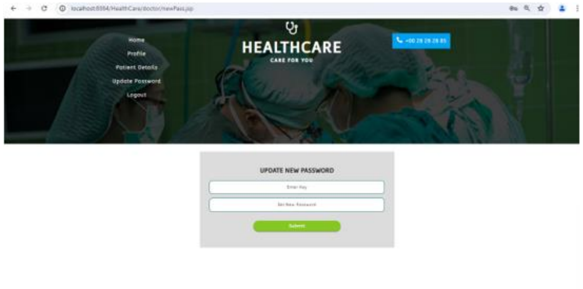


Figure 17: Doctor update password

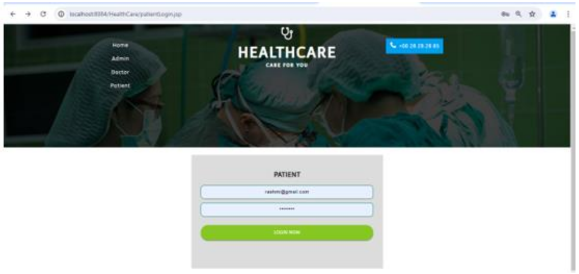


Figure 18: Patient login page

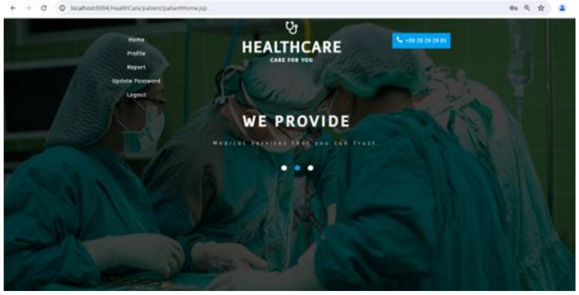
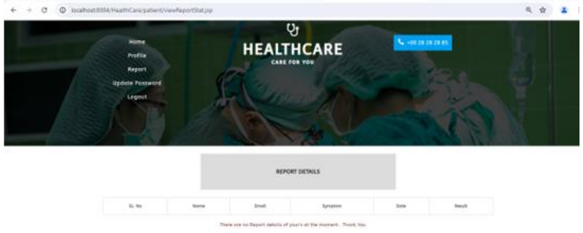


Figure 19: Patient Home page



SL. No	Name	Email	Symptom	Date	Result

There are no Report details of your's at the moment . Thank You

Figure 20: Patient Report

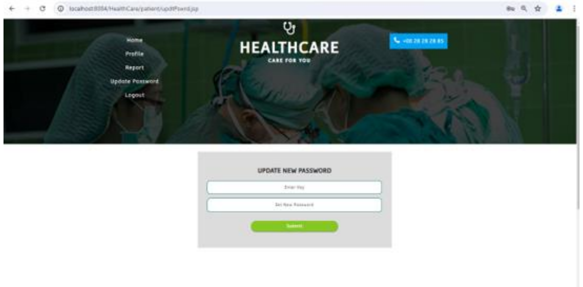


Figure 21: Update Password

CONCLUSION

The proposed system facilitates concurrent access to medical records by multiple stakeholders, including healthcare professionals, patients, and administrators. This system significantly reduces the need for physical storage space within healthcare facilities—a traditionally costly aspect of medical record-keeping. As the industry progresses toward a paperless environment, the proposed solution offers an efficient method for managing records that enhances data accuracy, optimizes space utilization, and promotes innovative record management practices.

By eliminating the necessity for patients to carry physical records, the system contributes to improved medication safety and minimizes redundant testing. It ensures that data capture, storage, and management are performed effectively, while also granting authorized personnel seamless access to patient information. Additionally, the system incorporates Advanced Encryption Standard (AES) encryption to safeguard patient data, thereby maximizing the system's benefits and ensuring the secure and efficient handling of sensitive medical information.

FUTURE ENHANCEMENT

The outcomes derived from this system are currently based solely on sample datasets. To achieve comprehensive evaluation across diverse classification scenarios, it is imperative to incorporate additional datasets, given the exponential growth and inherent dynamism of data in contemporary technological environments. Consequently, a thorough reclassification of the entire system is necessary, as results from previous methodologies have become outdated and no longer applicable.

Causal Productions has exerted considerable effort to maintain consistency in template appearance. However, a real-time system can be developed utilizing TensorFlow, a framework renowned for its efficacy in managing dynamic model operations. By aggregating datasets representing various classes, it is possible to enhance the model's capability to accurately identify a broader range of leaf types, thereby significantly improving classification precision.

REFERENCE

1. McDougall, J. Planning ahead for your company security. Inform. Quar., 1989, 5(3), 17-19.
2. Stephens, D.O. & Wallace, R.C. Electronic Records Retention: New strategies for data lifecycle management. Long-term data retention: Technical guidelines and best practices, 2003. 72-79.
3. Public Records Office of the UK National Archives. Management of electronic records. http://www. nationalarchives.gov.uk/documents/principles4.pdf (Retrieved on 15 April 2008).
4. Management Issues: Retention of Electronic Records, 1995. http://www.westchestergov.com/ wcarchives/electrnc.html#Adv (Retrieved on 25 February 2004).
5. Singapore National Eye Centre. News Archives: Singapore National Eye Centre achieves IRAS approved digital financial records in full compliance with the evidence act, 2003. http://www.snec.com. sg/news/press_archive_02072003.asp (Retrieved on 10 January 2008). 6. Coombs, P. The crisis in electronic government record keeping: A strategy for long-term storage. Library Computing, 1999, 18(3), 196-202.
6. McLeod, J. & Hare, C. How to manage records in the e-environments. Routledge, London, 2006. pp.14-18, 22-23.

7. McLean, T.R. Electronic medical record metadata: Do you know what’s in your record?. Inter. J. Controversial Medical Claims, 2008, 15 (1), 16-18.
8. Adobe PDF for Electronic Records: White Paper, 2007. http://www.adobe.com/government/pdfs/pdf_ electronic_records_wp.pdf (Retrieved on 10 April 2008).
9. Nelson, B. The electronic patient record: Pros and Cons. http://jimmy.qmuc.ac.uk/usr/im01nels/ Subjbook.htm#A (Retrieved on 15 May 2004).