GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

Private University Estd. in Karnataka State by Act No. 41 of 2013

PRESIDENCY GROUP OVER 40 YEARS OF ACADEMIC WISDOM

BANGALORE

A Project Report

On

“Confidentiality Of Patient Medical Records”

Batch Details

Sl. No.	Roll Number	Student Name
1	20201CSE0370	Bysani Lakshmi Narasimha Sai Lahari
2	20201CSE0386	SD Amruthavalli
3	20201CSE0416	Lingutla Thanusha

School of Computer Science,

Presidency University, Bengaluru.

Under the guidance of,

Dr. Prakash Shanmurthy

Assistant Professor

CONTENTS

1.ABSTRACT:

This paper addresses the security and privacy challenges associated with electronic Personal Health Records (PHRs) in cloud computing environments. As healthcare providers increasingly adopt PHRs to empower patients in managing their health data, concerns regarding the sensitive nature of this information become critical. Traditional encryption methods offered by commercial cloud platforms prove inadequate due to high key management overhead and maintenance costs. In response, this research introduces a novel approach based on Cipher Text Policy Attribute-Based Encryption (CP-ABE) and Proxy Re-Encryption (PRE). The proposed scheme ensures secure and fine-grained access control for outsourced PHRs, allowing owners to define access policies flexibly. The inclusion of a lightweight access policy update mechanism enhances adaptability. Additionally, a policy versioning technique is introduced to enable full traceability of policy changes. Through performance evaluation, the paper demonstrates the efficiency of the proposed scheme, providing a robust solution to the security and privacy challenges posed by outsourcing PHRs to cloud environments.

2.INTRODUCTION

In the realm of healthcare informatics, the management and sharing of Personal Health Records (PHRs) have grown increasingly complex as individuals and healthcare providers turn to third-party service providers, such as cloud storage systems, to store and manage valuable health data.While this outsourcing offers cost savings and efficient resource management, it also introduces significant privacy and security concerns. Typically, data owners opt to encrypt their sensitive health data before entrusting it to the cloud, a sensible measure to protect against unauthorized access.

However, encryption alone is insufficient to ensure the rigorous security control required in healthcare data management. Access control mechanisms become a critical necessity. Attribute-Based Encryption (ABE) has emerged as a powerful solution to this challenge, offering a 'one-to-many' encryption scheme with fine-grained access control. There are two primary types of ABE, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute-Based Encryption (KP-ABE). While CP-ABE is preferred from a security enforcement perspective due to its flexibility in policy definition, it comes with its own set of challenges, particularly related to overhead costs incurred during attribute revocation or policy updates. These complexities have significant implications, such as expensive ciphertext re-encryption and key management burdens that need to be efficiently addressed.

The proposed solution seeks to tackle these challenges by introducing a streamlined approach for updating CP-ABE access policies in the healthcare informatics domain, notably for sharing Personal Health Records (PHRs). Patients and data owners often wish to selectively share their health data with authorized parties, and to achieve efficient encryption and improved performance during data access and policy updates, the solution incorporates symmetric encryption to safeguard the data. The symmetric key, in turn, is encrypted using CP-ABE. What sets this approach apart is that policy updates primarily affect the encrypted symmetric key, obviating the need for re-encryption of all ciphertexts. This reduction in computational costs, especially at the proxy side, plays a pivotal role in improving the efficiency of healthcare data management. Additionally, the solution introduces a Proxy Re-Encryption (PRE) protocol to address the substantial cost associated with ciphertext re-encryption during policy updates, offering a well-considered strategy to ensure secure and efficient data sharing while navigating the complexities of healthcare informatics.

3. LITERATURE REVIEW

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω 0 , if and only if the identities ω and ω 0 are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption". In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model

Advantages:

1.User Empowerment: Effective policy update methods empower individuals to have greater control over who can access their personal health records, promoting patient autonomy.

2.Quick Access Modifications: Users can rapidly modify access policies, allowing for timely updates in the event of changing circumstances or preferences.

3.Improved Collaboration: Some methods facilitate secure sharing of health records among healthcare providers, promoting better care coordination and reducing duplication of tests and treatments.

4.Enhanced Accessibility: Policy updates can often be performed remotely, making it easier for individuals to manage their health information, even from a distance.

5.Reduced Administrative Burden: Lightweight methods minimize the administrative burden on healthcare organizations, allowing them to focus on patient care rather than complex policy management.

6.Efficient Record Sharing: They streamline the process of sharing health records with authorized parties, such as specialists or family members, ensuring faster access to critical information.

7.Customization: Many methods offer a high degree of policy customization, tailoring access levels for different categories of information and users.

8.Scalability: Effective methods can scale to accommodate a growing number of users and their health records without sacrificing performance or security.

Disadvantages:

1.Security Risks: Weak policy update methods can pose significant security risks, potentially leading to unauthorized data breaches and privacy violations.

2.Data Tampering: Inadequate methods may not adequately protect against data tampering or unauthorized alterations to health records, risking the integrity of the information.

3.Privacy Concerns: Some methods might not provide sufficient privacy safeguards, potentially allowing unauthorized parties to access sensitive health data.

4.Legal and Regulatory Compliance: Existing methods might not meet evolving legal and regulatory requirements, exposing healthcare organizations and individuals to compliance issues.

5.Complexity: Certain policy update methods can be complex to implement and use, potentially discouraging users from actively managing their health records.

6.Interoperability Challenges: There can be difficulties in ensuring interoperability between different systems and platforms, hindering seamless data sharing between healthcare providers and users.

7.Reliability: The reliability of certain lightweight methods can be inconsistent, leading to potential disruptions in policy management and data sharing.

8.Cost Implications: Implementing effective policy update methods may involve costs related to software, infrastructure, and staff training, which could be barrier for smaller healthcare providers or individuals with limited resources.

4. OBJECTIVES

User-Centric Application Design: Create a user-centric application that simplifies the process of updating access policies for personal health records. Focus on intuitive user interfaces and a seamless user experience to address the usability gaps identified in the literature survey.

Enhanced Security Features: Develop robust security features within the application to fortify data protection, including encryption, multi-factor authentication, and audit logs, addressing the security vulnerabilities identified in existing methods.

Interoperable Application: Design the application with interoperability in mind, enabling it to communicate and exchange data with other healthcare systems and platforms, reducing the interoperability challenges observed in the literature survey.

Compliance-Driven Framework: Integrate a compliance framework into the application to ensure it aligns with healthcare regulations and standards. Address the compliance issues identified in the literature survey, making it a reliable tool for healthcare organizations and individuals to maintain legal and regulatory adherence.

EXPERIMENTAL DETAILS/METHDOLOGY

HARDWARE SPECIFICATIONS:

• Processor	:	I3/Intel Processor
• RAM	:	8GB (min)
• Hard Disk	:	128 GB
• Key Board	:	Standard Windows Keyboard
• Mouse	:	Two or Three Button Mouse
• Monitor	:	Any

SOFTWARE SPECIFICATIONS:

• Operating System	:	Windows 10
• Server-side Script	:	Python 3.6
• IDE	:	PyCharm, VSCode.
• Libraries Used	:	Pandas, MYSQL
• Framework	:	Flask.

5. EXISTING METHODS:

Existing commercial cloud platforms usually provide symmetric or public key encryption as an optional feature to support data confidentiality for their tenants. However, such traditional encryption schemes are not suitable for data outsourcing environment because of high key management overhead of symmetric encryption and high maintenance cost for handling multiple copies of cipher text for public key encryption solution.
Drawbacks:

- High complexity.
- Low Computation.
- Requires skilled persons

6. PROPOSED METHOD:

Our proposed scheme is based on the cipher text policy attribute-based encryption (CP-ABE) and proxy re-encryption (PRE). In addition, we introduce a policy versioning technique to support the full traceability of policy changes. Finally, we conducted the performance evaluation to demonstrate the efficiency of the proposed scheme

Advantages:

- Accuracy is good.
- Low complexity.
- High Computation.
- No need of skilled persons

7. ARCHITECTURE DIAGRAM:

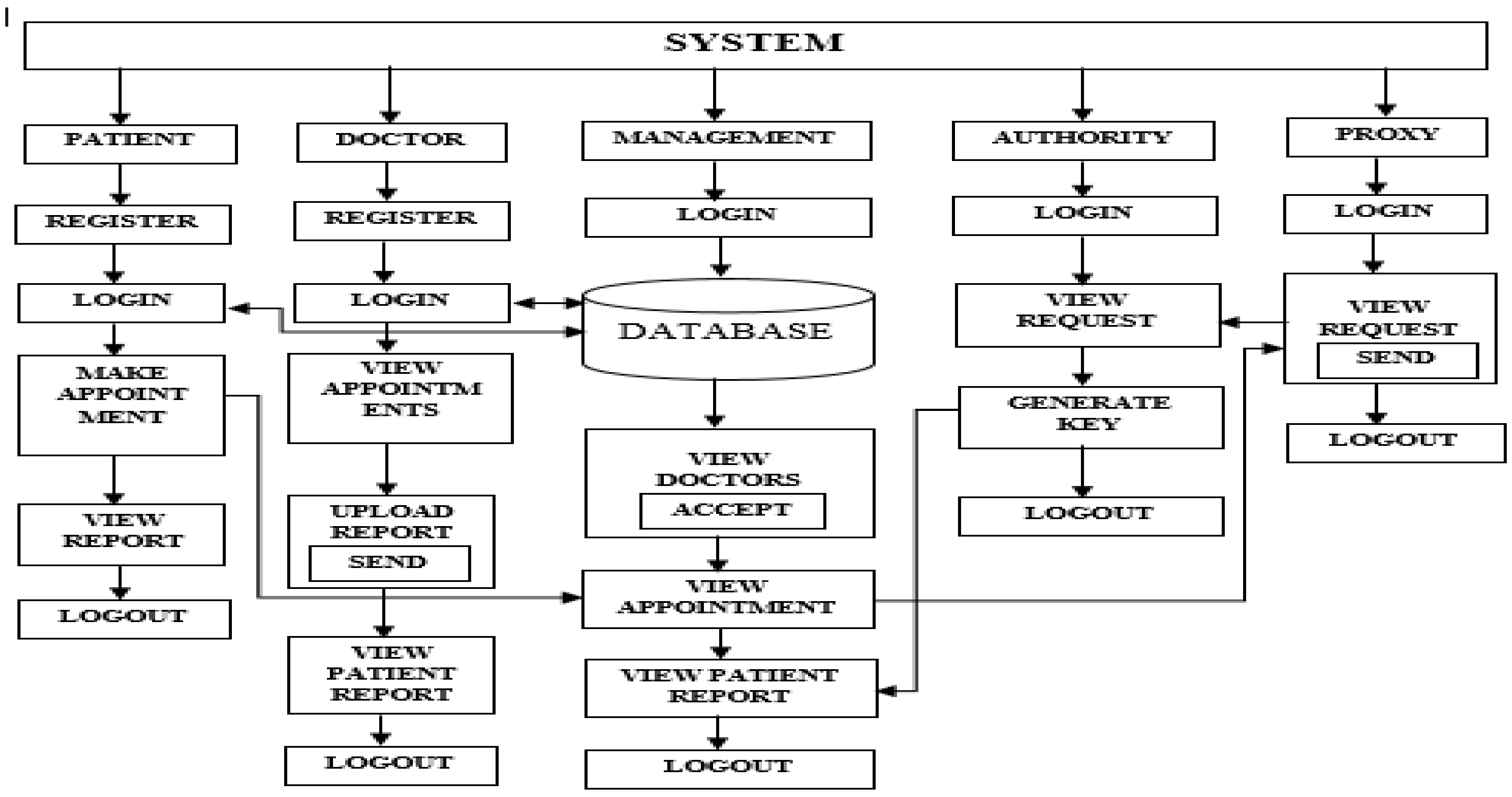


Fig 1

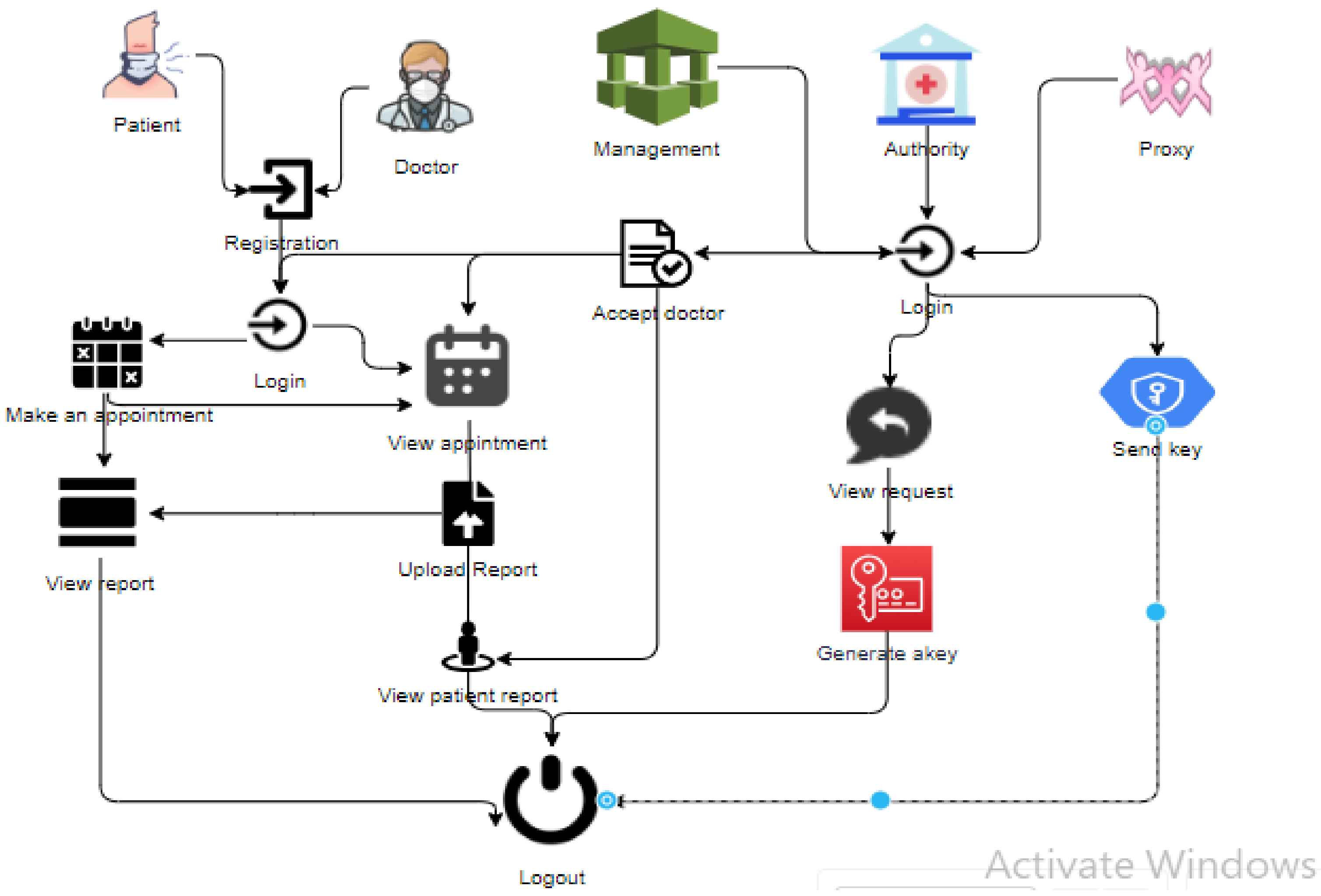


Fig 2

8. MODULES:

PATIENT:

- **Login**: Patient has to login with valid details which are used in his / her Registration.
- **Register:** Each and every patient has to register**.**
- **Appointment:** Patient will raise an appointment with symptoms.
- **View Report:** Patient will view reports after his / her medical checkup. Medical Records of every Hospitals must be visible using there generated key.
- **View health history:** patient can view their previous health data.
- **Logout:** Finally, logout from the system.

AUTHORITY:

- **Login:** Authority will login with default details
- **View Request:** View all requests from proxy.
- **Generate Key:** Generate Key to pass it to the authorized patient
- **Logout:** Finally logout from the system.

PROXY SERVER:

- **Login:** Authority will login with default details**.**
- **Send Request:** Pass requests to the authority.
- **Logout:** Finally logout from the system.

DOCTOR:

- **Login:** Doctor has to login with valid details which are used in his / her Registration.

- **Register**: Each and every patient has to register and management has to accept request.
- **View Appointment:** View all the appointments
- **Upload Report:** Uploads report.
- **Send File:** Send's file to the proxy
- **View Patient Report:** patient will view all the reports of the patient.
- **Logout:** Finally, logout from the system.

- **HOSPITAL MANAGEMENT:**
- **Login:** Management will login with default details, they can view the patients' medical details without any key.
- **Appointment:** Views all the appointments requests from the Patients
- **View Doctor Request:** View all the doctor requests who are registered.
- **Send Information:** Patient request will be passed to doctor
- **View Report :**View Patient Report in Emergency cases.
- **Logout:** Finally logout from the system.

9. METHODOLOGY:

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that plays a crucial role in securing data. It was established as a standard by the U.S. National Institute of Standards and Technology (NIST) in 2001 and has since become a global standard for data encryption.

1. Symmetric Encryption:

AES is a symmetric key encryption algorithm, which means that the same key is used for both encryption and decryption. This key must be kept secret between the sender and the recipient.

2. Key Lengths:

AES supports key lengths of 128, 192, and 256 bits, making it highly versatile and suitable for a wide range of security requirements.
The security of AES increases with longer key lengths.

3. Block Cipher:

AES is a block cipher, which means it operates on fixed-size blocks of data. The standard block size for AES is 128 bits (16 bytes).

4. Encryption Rounds:

AES operates in a series of rounds, with the number of rounds depending on the key length. For 128-bit keys, it uses 10 rounds; for 192-bit keys, it uses 12 rounds; and for 256-bit keys, it uses 14 rounds.

5. Substitution-Permutation Network:

Each round of AES consists of a series of transformations, including substitution (SubBytes), permutation (ShiftRows), and mixing (MixColumns).
These operations create confusion and diffusion within the data, making it

resistant to cryptographic attacks.

6. Key Expansion:

AES employs a key expansion algorithm to generate round keys from the original encryption key. These round keys are used in each round of the encryption process.

7. Security:

AES is considered highly secure and is widely used for protecting sensitive information, including government and military data, financial transactions, and communication over the internet.
The security of AES is based on its key length, with longer keys providing greater resistance to brute force attacks.

8. Performance:

AES is known for its efficiency and speed, making it practical for use in a wide range of applications, including software, hardware, and even resource-constrained devices.

9. Resistance to Cryptanalysis:

AES has withstood extensive cryptanalysis and is considered highly resistant to known attacks, including differential and linear cryptanalysis.

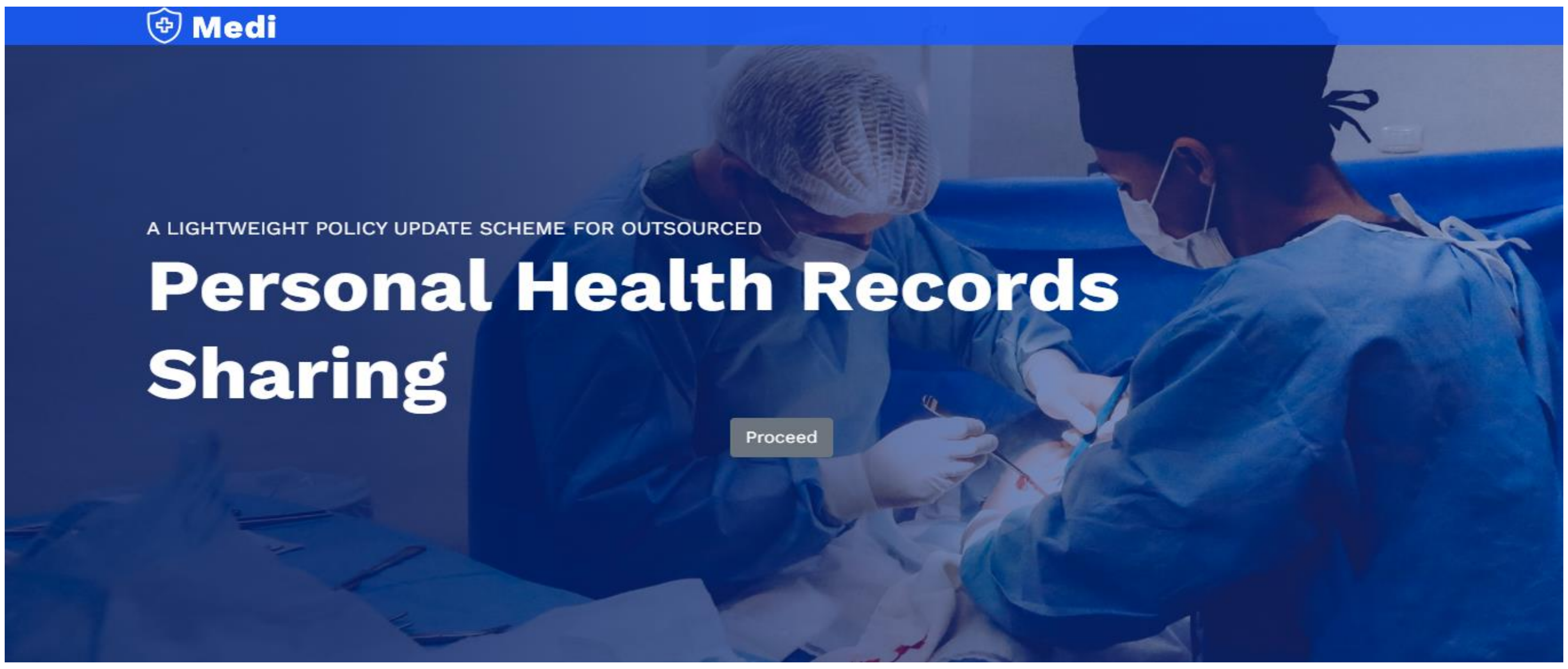
10. Standardization:

AES is an international standard adopted by governments, industries, and organizations worldwide, providing a consistent and trusted encryption method.

In summary, AES is a symmetric encryption algorithm that provides a high level of security, performance, and standardization. Its versatility in supporting multiple key lengths makes it suitable for various security requirements, and its resistance to cryptographic attacks has solidified its position as a fundamental tool for data protection in the digital age.

10. OUTCOMES:

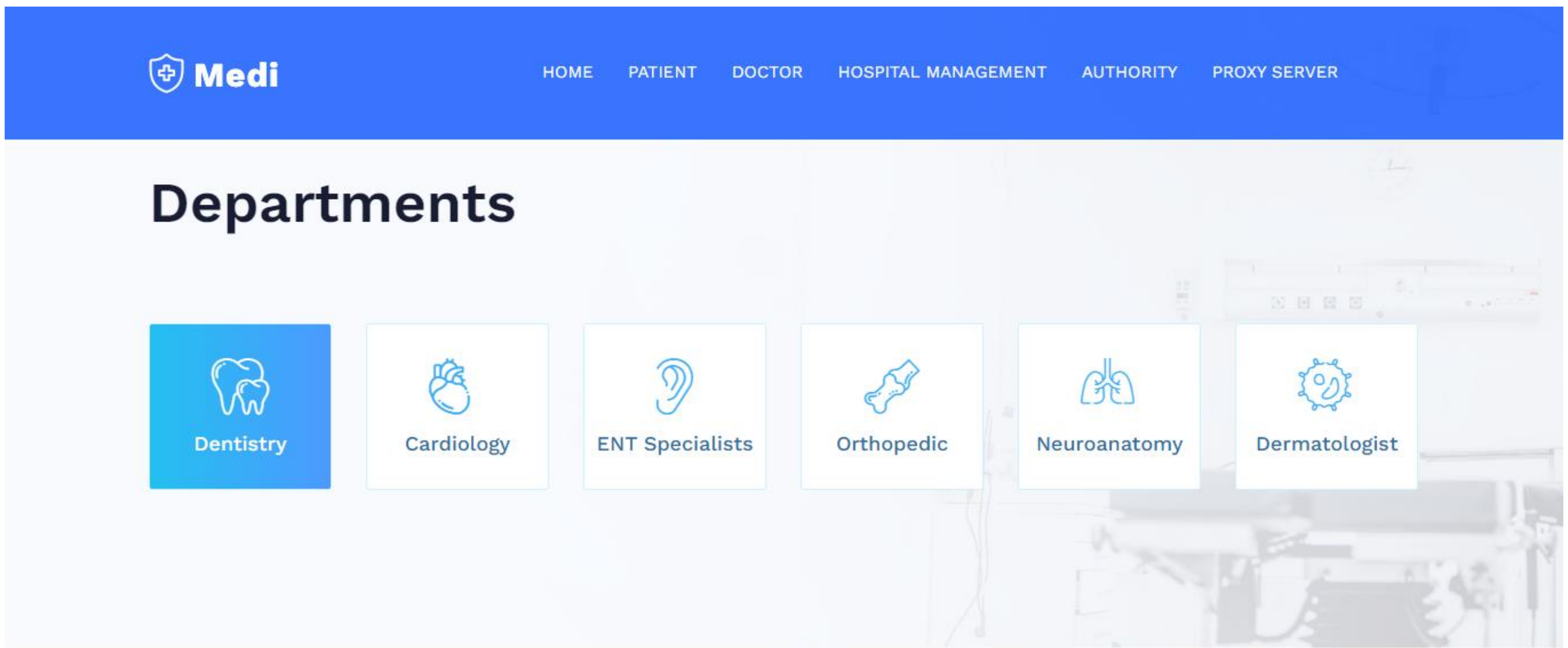
HOME PAGE:



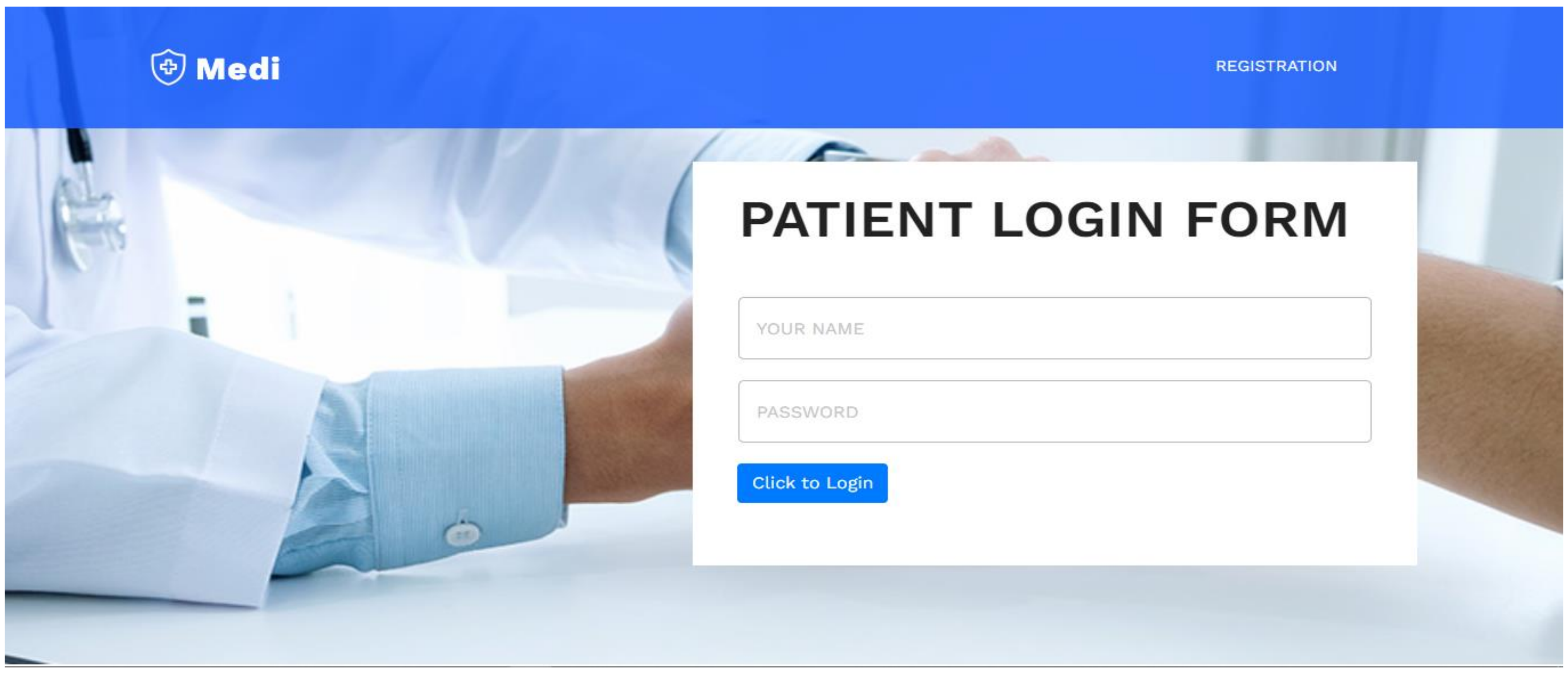
A LIGHTWEIGHT POLICY UPDATE SCHEME FOR OUTSOURCED

Personal Health Records Sharing

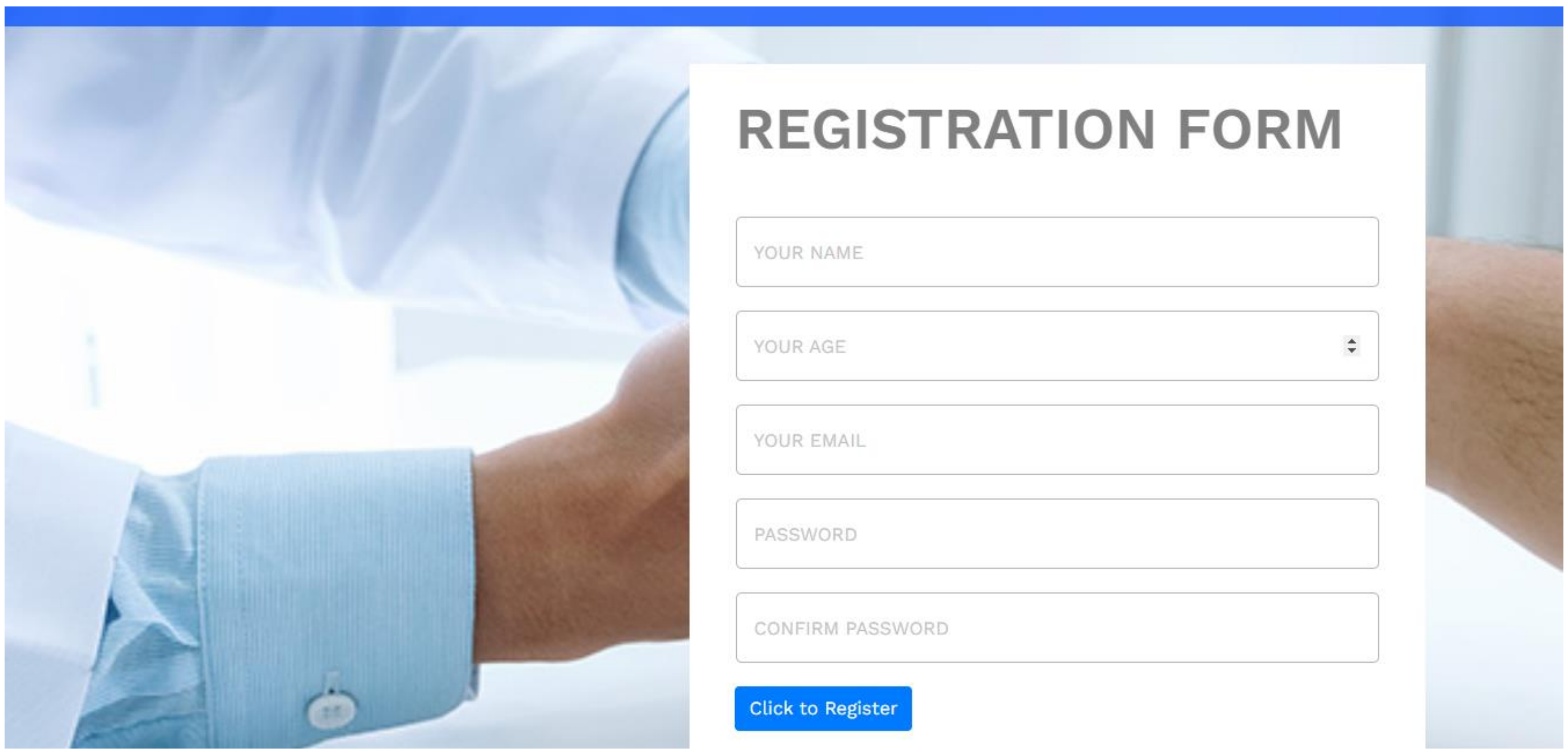
MODULES PAGE:



PATIENT LOGIN FORM:

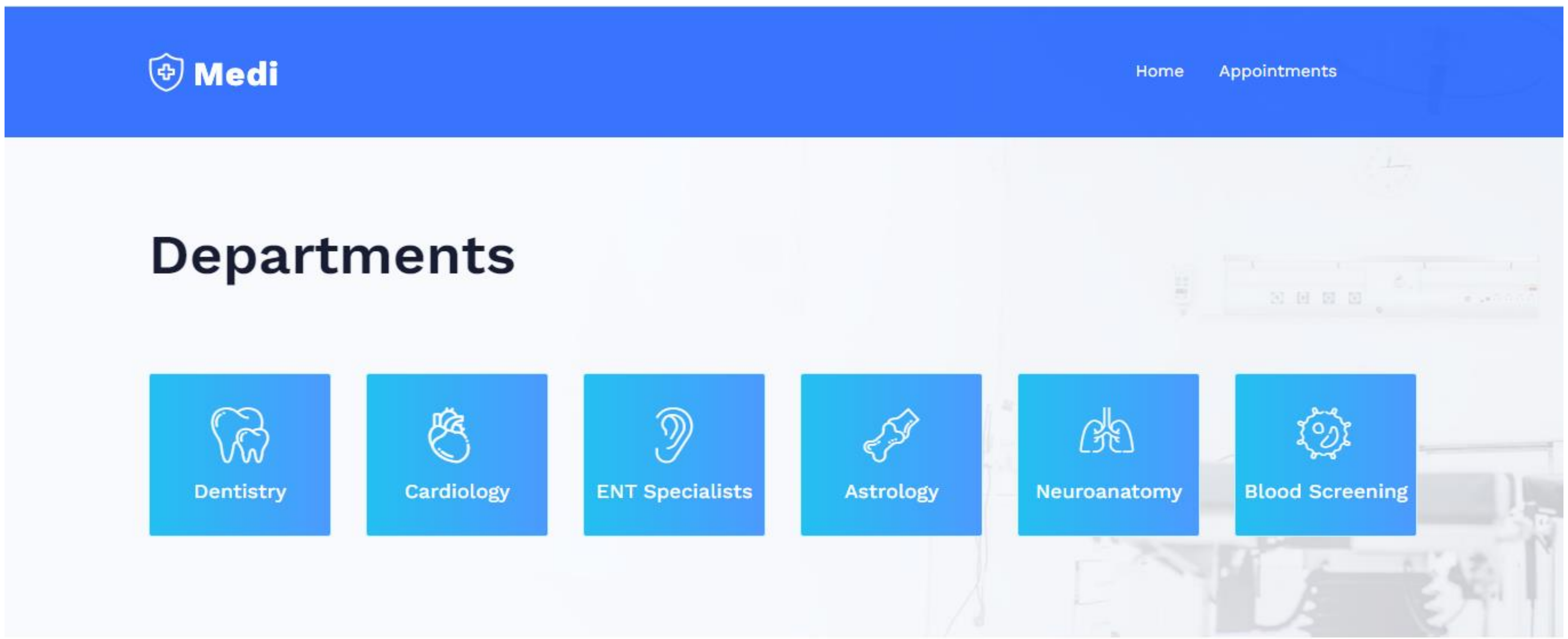


PATIENT REGISTRATION FORM:



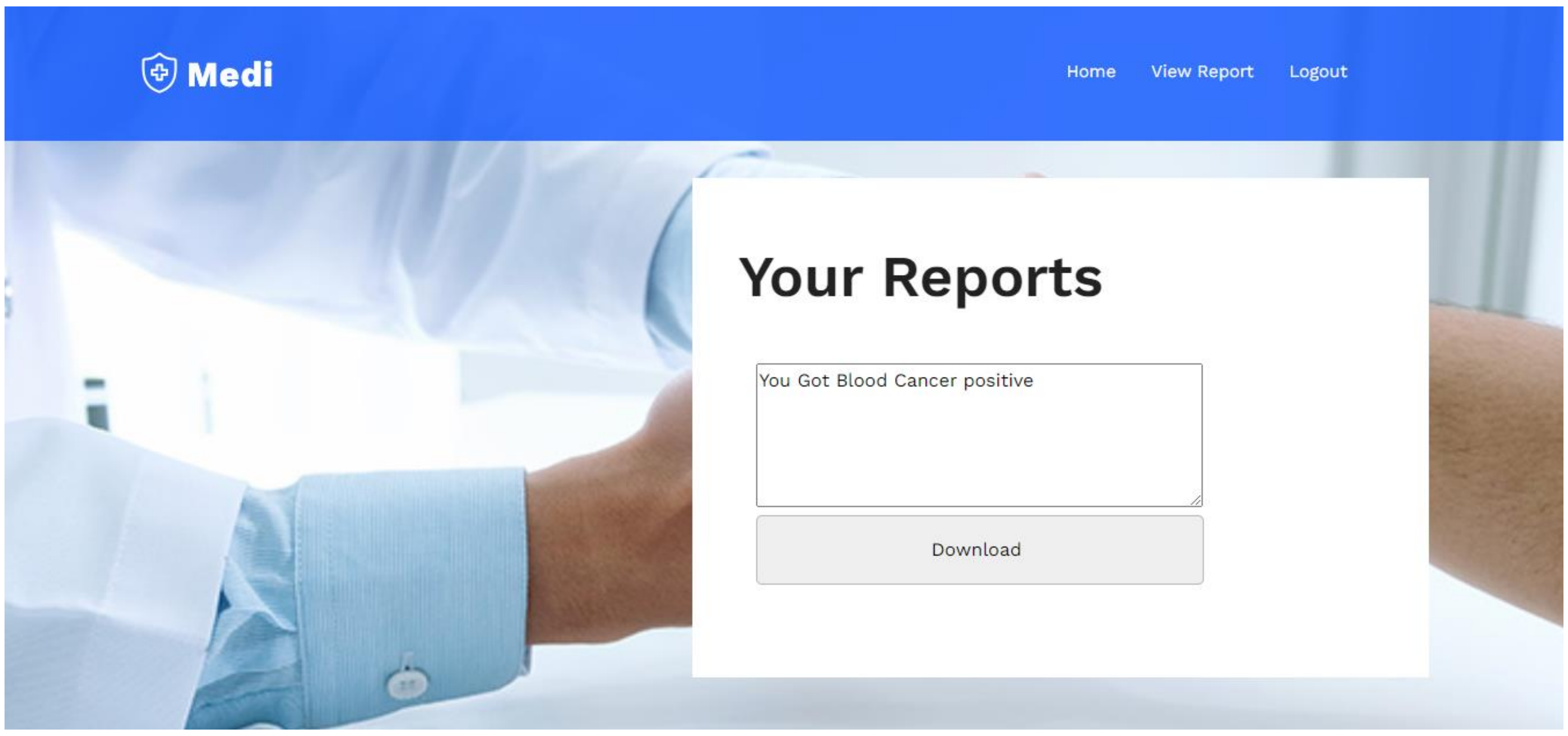
REGISTRATION FORM

MANAGEMENT HOME PAGE:



Departments

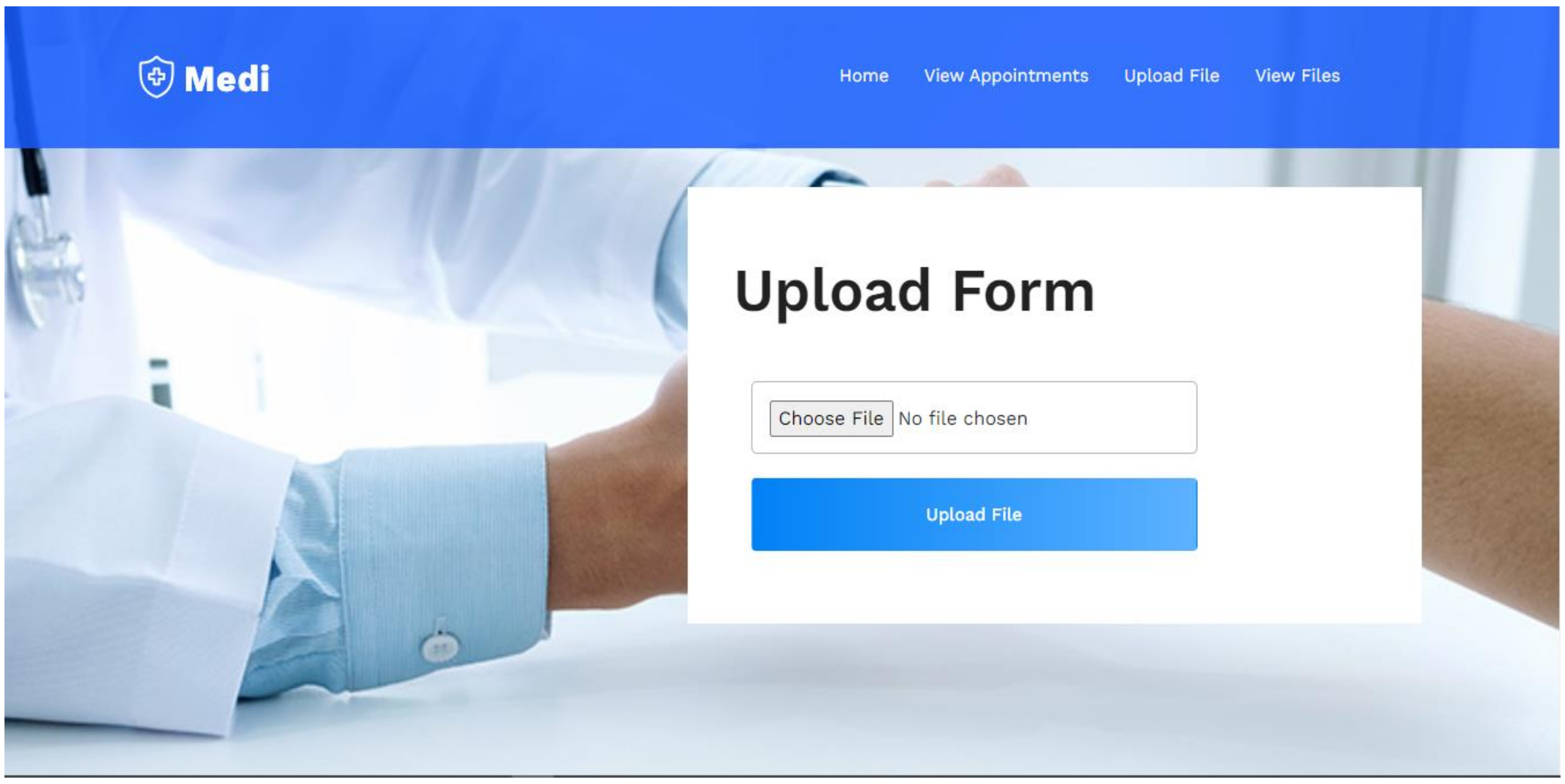
VIEW REPORT:



Your Reports

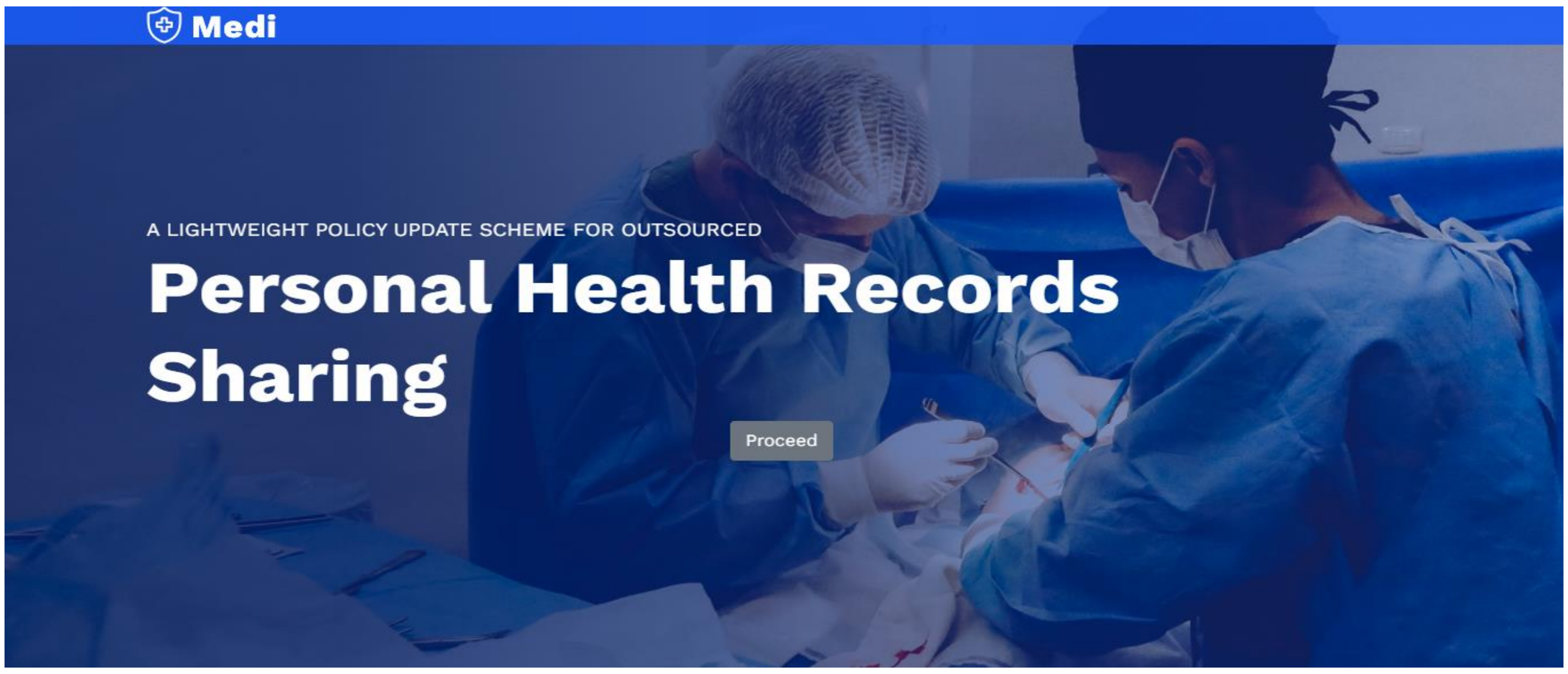
You Got Blood Cancer positive

UPLOAD FILES:



Upload Form

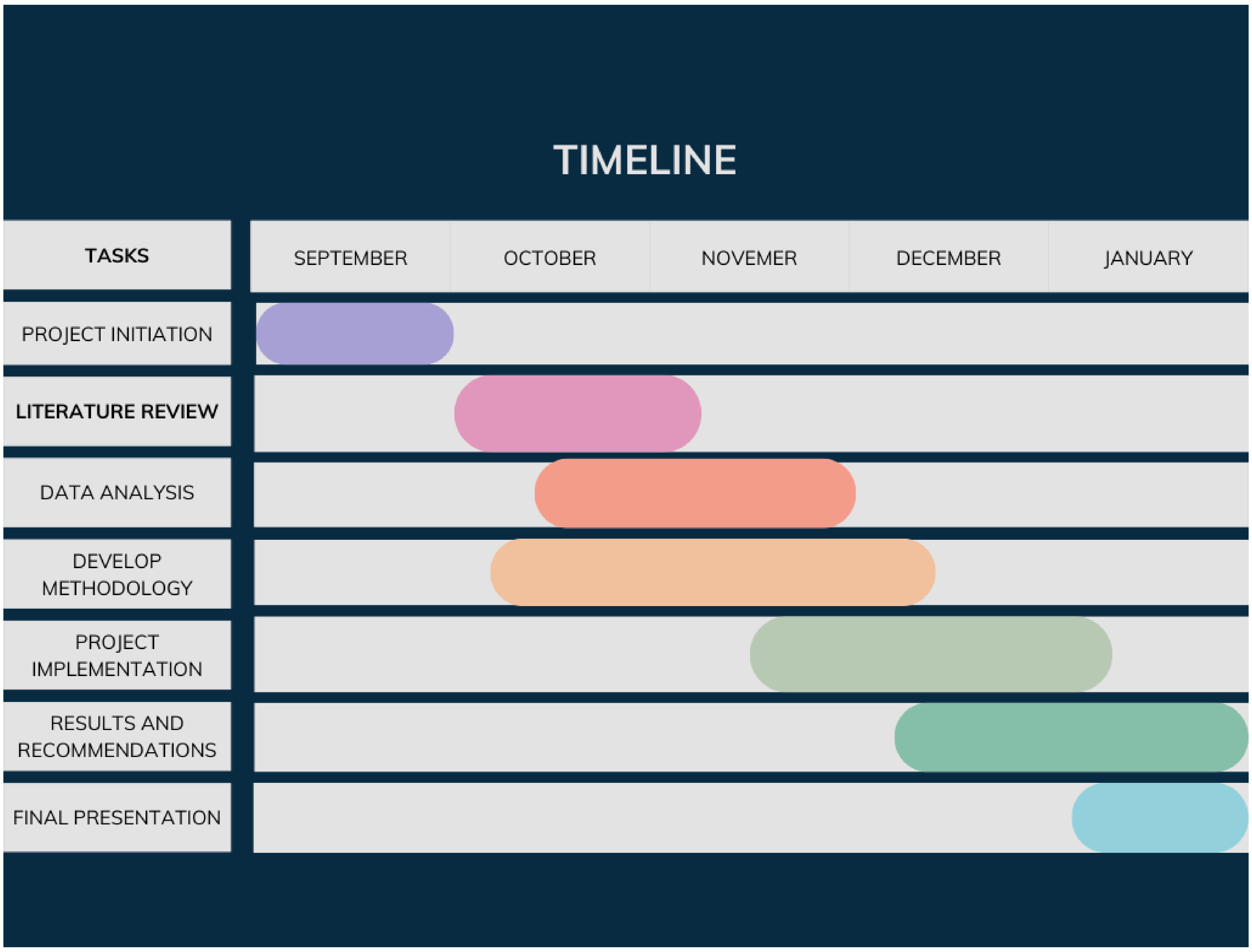
LOGOUT:



A LIGHTWEIGHT POLICY UPDATE SCHEME FOR OUTSOURCED

Personal Health Records Sharing

11. TIMELINE OF THE PROJECT/ PROJECT EXECUTION PLAN



12. CONCLUSION

Your innovative policy update scheme employs policy outsourcing and proxy re-encryption, offloading costs to the server and enhancing scalability. A user-friendly GUI tool facilitates CP-ABE policy updates, allowing encrypted file and policy uploads to outsourced storage without local database retrieval. The web-based tool enables transparent access control, allowing policy updates from anywhere. A policy versioning technique efficiently reconstructs historical policies for rigorous auditing. Demonstrations indicate superior file re-encryption performance with multi-thread processing. Overall, your approach provides an efficient, scalable, and user-friendly solution for transparent access control and policy management.

13. REFERENCES

[1] A. Sahai and B. Waters, ‘‘Fuzzy identity-based encryption,’’ in Proc. 24th Annu. Int. Conf. Appl. Cryptograph. Technique (EUROCRYPT) (Lecture Notes in Computer Science). Berlin, Germany: Springer, May 2015, pp. 457–473.

[2] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, May 2007, pp. 321–334.

[3] L. Cheung, J. Cooley, R. Khazan, and C. Newport, ‘‘Collusion resistant group key management using attribute-based encryption,’’ Cryptol. ePrint Arch., Tech. Rep. 2007/161. [Online]. Available: https://eprint.iacr.org/2007/161.pdf

[4] S. Belguith, N. Kaaniche, and G. Russello, ‘‘PU-ABE: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT,’’ in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 924–927.

[5] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, J. Chen, and Z. You, ‘‘An efficient attribute-based encryption scheme with policy update and file update in cloud computing,’’ IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6500–6509, Dec. 2019.

[6] M. Mambo and E. Okamoto, ‘‘Proxy cryptosystems: Delegation of the power to decrypt cipher texts,’’ IEICE Trans., vol. E80-A, no. 1, pp. 54–63, 1997.

[7] K. Liang, W. Susilo, and J. K. Liu, ‘‘Privacy-preserving cipher text multisharing control for big data storage,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1578–1589, Aug. 2015. [8] S. Fugkeaw and H. Sato, ‘‘Embedding lightweight proxy re-encryption for efficient

attribute revocation in cloud computing,'' J. High Perform. Comput. Netw., vol. 9, no. 4, pp. 299–309, 2016.

[9] Y. Kawai, ''Outsourcing the re-encryption key generation: Flexible ciphertext-policy attribute-based proxy re-encryption,'' in Proc. Int. Conf. Inf. Secur. Pract. Exper. (ISPEC), Beijing, China, 2015, pp. 301–315.

[10] X. Liang, Z. Cao, H. Lin, and J. Shao, ''Attribute based proxy re-encryption with delegating capabilities,'' in Proc. 4th Int. Symp. Inf., Comput., Commun. Secur. (ASIACCS), 2009, pp. 276–286.

[11] L. Touati and Y. Challal, ''Instantaneous proxy-based key update for CPABE,'' in Proc. IEEE 41st Conf. Local Comput. Netw. (LCN), Dubai, United Arab Emirates, Nov. 2016, pp. 591–594. [12] K. Yang, X. Jia, K. Ren, R. Xie, and L. Huang, ''Enabling efficient access control with dynamic policy updating for big data in the cloud,'' in Proc. IEEE Conf. Comput. Commun. (INFOCOM), Apr. 2014, pp. 2013–2021.

[13] K. Yang, X. Jia, and K. Ren, ''Secure and verifiable policy update outsourcing for big data access control in the cloud,'' IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec. 2015.

[14] S. Fugkeaw and H. Sato, ''Scalable and secure access control policy update for outsourced big data,'' Future Gener. Comput. Syst., vol. 79, pp. 364–373, Feb. 2018.

[15] L. Cheung and C. Newport, ''Provably secure ciphertext policy ABE,'' in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Richmond, VI, USA, Oct. 2007, pp. 456–465.