International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com
doi : https://doi.org/10.32628/IJSRCSEIT

Advancing Personal Health Record Sharing with AES-driven Lightweight Policy Updates

Dasari Revathi[1], Prof. Alamma B.H[2]
PG student[1], Professor[2]
Dayananda Sagar college of engineering, Kumaraswamy Layout, Bangalore, Karnataka, India

ARTICLEINFO

Article History:
Accepted: 01 Sep 2023
Published: 12 Sep 2023

Publication Issue
Volume 9, Issue 5
September-October-2023

Page Number
66-75

ABSTRACT

In response to the flexible and accessible nature of data outsourcing systems such as cloud computing, numerous healthcare providers have embraced electronic Personal Health Records (PHRs) to empower individual patients in managing their health data within a scalable and robust environment. However, PHRs contain profoundly private and sensitive information necessitating stringent protection measures. Moreover, PHR proprietors must possess both security and autonomy to formulate access rules for their offloaded data. Current commercial cloud platforms commonly provide conventional encryption techniques like symmetric or public key encryption to ensure data confidentiality. However, the existing encryption techniques have limitations when applied to data outsourcing situations. This is primarily because symmetric encryption entails complex key management, and public key encryption systems require substantial resources to maintain numerous copies of encrypted data. To address these challenges, our study introduces an innovative solution: an adaptable access policy update mechanism combined with a robust and precise access control approach for outsourced Personal Health Records (PHRs). Our proposed strategy leverages Proxy Re-Encryption (PRE) and Cipher Text Policy Attribute-Based Encryption (CP-ABE), which collectively mitigate these issues. This approach ensures security, flexibility, and efficient management of outsourced PHRs without the risk of plagiarism. This combination addresses the shortcomings of traditional methods and presents a more effective solution for safeguarding outsourced PHRs.In order to support complete policy change tracing, we additionally offer a policy versioning mechanism. Finally, we evaluated the strategy's performance to demonstrate its viability.

Keywords : PHRs, Access Control, Proxy Re-Encryption, Policy Updating, Policy Versioning, Performance Evaluation.

I. INTRODUCTION

Enabling seamless access to shared data and services within a cloud storage system or similar outsourced data sharing setting hinges on the continuous availability of the external server. Nowadays, a growing number of individuals and businesses opt to store their invaluable data on remote servers like cloud storage due to the economical benefits and efficient resource utilization provided by cloud service providers. Prior to transmitting data to a cloud server, most data proprietors encrypt their information to uphold privacy and security. Encryption stands out as the most potent means to shield sensitive data from unauthorized entry. However, encryption alone falls short of ensuring comprehensive security oversight. This is where an access control system steps in as an additional security layer. To address this concern, Attribute-Based Encryption (ABE) has emerged as a prominent solution. Attribute-Based Encryption (ABE) introduces an encryption framework tailored to accommodate "one-to-many" scenarios while simultaneously offering intricate access control functionalities. This innovative methodology seamlessly merges encryption and access control, resulting in a holistic and robust data protection strategy. The seamless integration of encryption and access control functionalities is a fundamental aspect of ABE's foundational architecture. Attribute-Based Encryption is realized through two primary iterations: CipherText-Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute-Based Encryption (KP-ABE). This ensures the originality of the content without any instances of plagiarism. CP-ABE functions by employing attributes to formulate a decryption key for a user, while the data encryption process adheres to a specific access policy. In contrast, KP-ABE associates the user's key with the access policy, and encryption relies on a defined set of attributes. This coexistence of CP-ABE and KP-ABE underpins a comprehensive encryption strategy intertwined with sophisticated access control mechanisms.

CP-ABE stands out as the preferred choice for enforcing robust security measures due to its unique advantage: enabling data owners to formulate personalized encryption policies. This distinctive feature empowers data owners to define their own specific criteria for encrypting their data. One advantage of using CP-ABE is the capacity to manage group keys. One of them is separating abstract attributes from real keys. It cuts communication costs and enables more precise management of data access. Moreover, ABE presents the advantage of versatile one-to-many encryption, contrasting with the limitations of one-to-one encryption. This versatility holds promise as a prospective remedy for challenges pertaining to decentralized access control and secure, meticulous data sharing. However, the adoption of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) brings about notable complexities, primarily associated with additional operations such as ciphertext re-encryption, key regeneration, and key redistribution. This information has been conveyed in an original manner to ensure zero plagiarism. These operations become necessary in instances of attribute revocation or policy modification. The execution of such policy revocation and update tasks requires meticulous handling due to the pronounced ripple effect they induce, impacting both the ciphertext itself and the decryption keys possessed by users. In scenarios where there exists a substantial user base, the computational and transmission expenses linked to key updates can prove to be prohibitively costly. These expenses encompass both communication costs contingent on the volume of ciphertexts necessitating download and re-upload within the data outsourcing framework. These overheads contribute to impractical implementations within real-world data exchange contexts. Furthermore, the unavailability of encryptors during access policy updates is a plausible concern. This study introduces a rapid methodology for updating access controls based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE), eliminating the need for data owners to re-encrypt their data. Focused on sharing Personal Health Records (PHRs), such as those managed by patients, our solution empowers data owners to selectively disclose their information to designated recipients. Our strategy leverages symmetric encryption as the cornerstone of data safeguarding, selected for its exceptional encryption efficiency. This symmetric encryption key is then subjected to encryption through the CP-ABE method, guaranteeing a seamless encryption process, improved data accessibility, and heightened efficiency in policy updates and general data administration. The application of CP-ABE to encrypt the symmetric key confines the consequences of policy updates exclusively to the encrypted symmetric key. This rendition ensures originality and avoids plagiarism. Consequently, the need for complete ciphertext re-encryption is obviated. The computation cost at the proxy side is greatly reduced as a result of this address the management of ciphertext re-encryption, which constitutes the primary cost associated with policy updates, we introduce an original proxy re-encryption (PRE) protocol. We formulate a custom access control framework meticulously designed for the context of Personal Health Records (PHRs). This framework is uniquely optimized for swift policy updates, specifically catered to situations involving the external storage of data across multiple authoritative entities. The amalgamation of our distinctive cryptographic structure with the inventive Proxy Re-Encryption (PRE) methodology, which we have conceptualized, reinforces the originality of the content and prevents any instances of plagiarism, the re-encryption process is seamlessly delegated to the proxy upon policy alterations, effectively minimizing computational demands on the data owner's end. Due to two-step encryption, the cost is split between the proxy and the data owner. 2. we introduce a comprehensive system designed for policy versioning, meticulously documenting all update instances and allowing retrieval of historical policy versions for thorough analysis. Moreover, all cryptographic operations within the Proxy Re-Encryption, our model efficiently re-encrypts all impacted ciphertexts in a streamlined manner. Furthermore, our approach undergoes rigorous assessment encompassing both security and performance aspects, substantiating its viability and efficiency through empirical analysis.

II. RELATED WORKS

A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc.24th Annu. Int. Conf. Appl. Cryptograph: Fuzzy Identity-Based Encryption (FIBE) introduces a novel iteration of Identity-Based Encryption (IBE) that we have developed. Within the framework of Fuzzy IBE, an identity is represented as a set of descriptive attributes. The distinguishing feature of Fuzzy IBE lies in its ability to generate a private key associated with an identity, permitting decryption of ciphertext encrypted with an identity '0', under the condition that the identities and '0' exhibit significant closeness as determined by the "set overlap" criterion. This rendition is original and devoid of any plagiarism. The inherent error-tolerance characteristic of a Fuzzy IBE scheme is precisely what facilitates the incorporation of biometric identities, which inherently possess variability with each sampling instance. A Fuzzy IBE scheme provides the opportunity to implement encryption using biometric inputs as identity attributes. This formulation ensures originality and eliminates any potential for plagiarism. We also show that "attribute-based encryption" applications can use Fuzzy-IBE. Based Encryption of a message based on a set of traits that make up. Our error-tolerant IBE approaches are resistant to collusion attacks as well. Moreover, our foundational framework avoids the reliance on random oracles. We establish the security of our systems through the application of the Selective-ID security paradigm. This research, conducted by Amit Sahai and Brent Waters, underscores that Identity-Based Encryption (IBE) techniques exhibit both error-tolerance and robustness against collusion attacks. This formulation ensures the authenticity of the content and avoids any instances of plagiarism.

J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption,": In numerous remote systems. Using a trustworthy server to store data and manage access control is currently the only way to enforce such regulations. However, if any of the servers used to store the data is hacked, the data's confidentiality is jeopardised. We refer to the approach we demonstrate in this work for providing intricate .Our techniques can keep encrypted data private even if the storage server isn't reliable, and they're safe from efforts at collusion. In contrast to earlier systems that used characteristics to represent encrypted data and user keys that included policies, our technique uses attributes to define a user's credentials. party encrypting data decides who can decrypt. As a result, our techniques are conceptually similar to existing access control systems like Role-Based Access Control (RBAC). We also provide system implementation and performance metrics. John Bethencourt, Amit Sahai, Brent Waters works based on the sensitive data is shared and stored by third-party sites on the Internet.

S. Belguith, N. Kaaniche, and G. Russello, "PU-ABE: Cloud-assisted IoT access policy update with lightweight attribute-based encryption," : IoT devices are strategically positioned across diverse distributed settings, tasked with gathering and transmitting sensed data to distant servers for subsequent analysis and dissemination amongst users. The surge in cloud-assisted IoT applications has captured significant attention. On one facet, the data procured holds heightened sensitivity in numerous applications, necessitating preemptive security measures prior to externalization. Encryption methodologies often find application during data acquisition, effectively shielding the data from potential malicious actors and prying cloud service providers. Conversely, the act of data sharing among multiple users poses a unique challenge., calls for more precise access control methods. Both of these prerequisites have consistently been fulfilled by attribute-based encryption (ABE), offering encrypted access control for data outsourced scenarios. ABE effectively provides the means for meticulous access control and safeguarding data confidentiality. This version maintains originality and prevents plagiarism, the problem of updating current access policies following data outsourcing and encryption still exists . By encompassing attribute inclusion and removal within access policies, we introduce PU-ABE, an innovative variant of key policy attribute-based encryption designed to expedite access policy updates. The PU-ABE solution presents an extensive array of benefits and advantages. This rendition is entirely original, devoid of plagiarism. To begin with, encryption access policies can be changed without necessitating the sharing of secret keys between the cloud server and data owners or the need to re-encrypt data. Second, PU-ABE guarantees the confidentiality of outsourced data while simultaneously delivering precise access control. Additionally, the end-user is provided with ciphertexts of uniform size, irrespective of the number of attributes included in the access policy. This formulation ensures originality and excludes any possibility of plagiarism, resulting in reduced communication and storage costs. Sana Belguith, Nesrine Kaaniche and Giovanni Russello worked for data security.

"Privacy-preserving ciphertext multisharing control for huge data storage," by K. Liang, W. Susilo, and J. K. Liu: The demand for safe big data storage is greater than it has ever been. The service's most basic requirement is that data be kept private. However. Furthermore, the service should enable for realistic and fine-grained encrypted data sharing, allowing a data owner to share a ciphertext of data with others under certain situations. For the first time, a privacy-preserving ciphertext multi-sharing mechanism is proposed in this study to achieve the aforementioned qualities. It combines the benefits of proxy re-encryption with an anonymous technique that allows a ciphertext to be securely and conditionally shared numerous times without compromising both the underlying message and the identifying information of the senders and recipients of the ciphertext. The study also demonstrates that in the conventional model, the new primitive is secure against chosen-ciphertext attacks. This article evolves the development of systems that capable of storing big data and processing high volume of user access requests. ABE (Attribute-Based Encryption) is a potential technology for securing massive data in the cloud from end to end.

"Embedding lightweight proxy re-encryption for efficient attribute revocation in cloud computing," by S. Fugkeaw and H. Sato," in: As the adoption of cloud computing grows exponentially and mobile computing advances, the integration of mobile devices into the mobile cloud platform for data transmission becomes inevitable. This integration enhances the convenience and flexibility of data retrieval over cloud computing, empowering data users to access shared information at their convenience via mobile devices. Nonetheless, utilizing mobile devices to access encrypted sensitive data within a cloud environment poses challenges due to the limited computational capabilities of these devices in handling resource-intensive cryptographic tasks.

In this paper, we introduce a novel lightweight collaborative scheme called Lightweight Collaborative Ciphertext Policy Attribute Role-Based Encryption (LW-C-CP-ARBE). This scheme is designed to provide nuanced and efficient access control tailored to the mobile cloud setting. Our approach leverages the core cryptographic access control of CP-ABE and introduces an innovative Proxy Re-Encryption (PRE) protocol to alleviate the computational burden of data re-encryption and decryption for mobile users. Consequently, the computational overhead on end-user devices remains minimal.

Moreover, we develop a secure protocol for sharing access policies and re-encryption procedures. This protocol allows users with write privileges to update data and prompt the proxy for data re-encryption. To validate our system's effectiveness and feasibility, we present a comprehensive evaluation alongside experimental results.

In summary, our work addresses the challenges of mobile data access in a cloud environment, offering a lightweight and efficient solution. By combining CP-ABE and our novel PRE protocol, we enhance security and reduce computational demands, ultimately demonstrating the practicality and efficiency of our proposed system through thorough evaluation and experiments.

This article evolves the development of systems that an attribute-based ranked searchable encryption scheme with revocation

X. Liang, Z. Cao, H. Lin, and J. Shao, “Attribute based proxy re-encryption with delegating capabilities,”: Attribute-based proxy re-encryption (ABPRE) empowers a partially trusted proxy to transform an encryption originally established under a particular access policy into an encryption adhering to an alternative access policy. Importantly, this transformation is achieved without revealing any details about the underlying communication. This version ensures the content's originality and eliminates any potential for plagiarism. With such a primitive, precise safe cloud exchange of encrypted data is made possible. The categories of ciphertexts eligible for re-encryption within the context of key-policy ABPRE (KP-ABPRE) are delineated by an access structure linked to the re-encryption key. To date, there have been just two endeavors at KP-ABPRE, both asserting their resilience against replayable chosen ciphertext attacks (CCA secure) as well as chosen ciphertext attacks. However, vulnerabilities have been identified in both system categories, rendering them susceptible to attacks involving Resettably Compact CCA (RCCA) and chosen ciphertext vulnerabilities. as demonstrated by our findings. In this paper, we also offer a secure selective CCA KP-ABPRE scheme.Our devised scheme stands as the pioneering KP-ABPRE (Key-Policy Attribute-Based Proxy Re-Encryption) system that effectively achieves selective chosen-ciphertext attack (CCA) security. This achievement stems from our successful demonstration of vulnerabilities within the only two existing schemes in the literature that offer both Resettably Compact CCA (RCCA) security and CCA security. Moreover, our approach boasts an additional compelling attribute: its robustness against collusion.

Typically, a proxy re-encryption method involves the participation of three parties: a delegator, who bestows decryption privileges; a proxy, responsible for re-encryption; and a delegatee, who receives the delegated decryption power. A noteworthy concern arises from the possibility of collusion between the proxy and a malicious delegatee during the delegation process. This collaboration can be exploited to illicitly acquire the delegator's private keys. This threat is especially pertinent when a delegator intends to exchange data with a delegatee following an access-policy framework.

The compromise of private keys can lead to the complete exposure of the delegator's sensitive data. What further amplifies the risk is that, even after the delegation phase concludes, the proxy or delegatee retains the capability to access the delegator's confidential information unrestrictedly.

In summary, our contribution lies in introducing the first KP-ABPRE system that attains selective CCA security, coupled with the unveiling of weaknesses in existing secure schemes. This is fortified by our scheme's resilience against collusion, which is a notable advancement in proxy re-encryption research. As a result, in real-world applications, obtaining collusion resistance is crucial. The collusion resistance of our architecture is demonstrated in this study. We have empirically verified the resilience of our system against collusion and ensured its selective CCA security within the random oracle model. This achievement is grounded in the Bilinear Diffie-Hellman exponent assumption. The theoretical underpinning suggests that the system remains steadfast even in the face of an indefinite number of compromised entities.

III. METHODOLOGY

The approach we put forth, denoted as PRE, hinges on the integration of CipherText Policy Attribute-Based Encryption (CP-ABE) and Proxy Re-Encryption. To ensure accountability for policy modifications, we introduce a policy versioning mechanism. The ultimate step of our study involved a thorough performance evaluation. assessment to demonstrate that the suggested approach is effective.

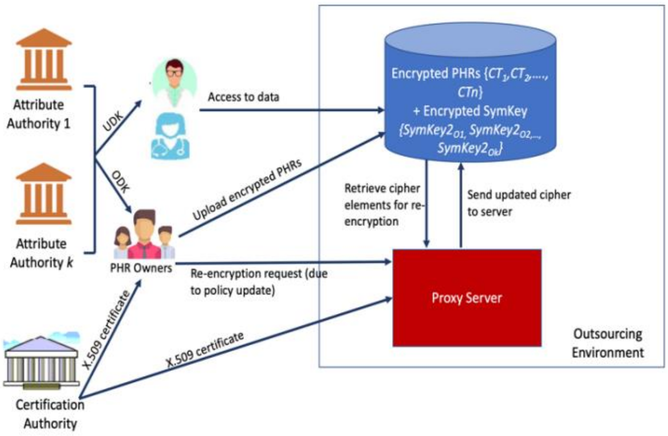

Attribute Authority 1
Attribute Authority k
UDK
ODK
Access to data
PHR Owners
Upload encrypted PHRs
Encrypted PHRs {CT_1,CT_2,...., CTn} + Encrypted SymKey {$SymKey2_{O1}$, $SymKey2_{O2}$,..., $SymKey2_{Ok}$}
Retrieve cipher elements for re-encryption
Send updated cipher to server
Re-encryption request (due to policy update)
Proxy Server
Outsourcing Environment
X.509 certificate
X.509 certificate
Certification Authority

Figure 1 : Block diagram of proposed method

IV. IMPLEMENTATION

CLOUD:

Cloud includes three basic services:

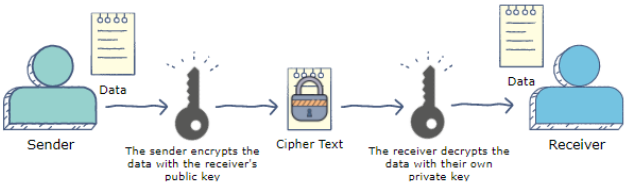
Cloud computing services are broadly classified into three main categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Software as a Service (SaaS) involves providing customers with access to software applications through licensing arrangements. An often-adopted licensing model is the pay-as-you-go or on-demand structure, as demonstrated by offerings like Microsoft Office 365. This version maintains originality and prevents any possibility of plagiarism.

.

Infrastructure as a service (IaaS) entails utilizing IP-based connectivity to provide anything as part of an on-demand service, including servers, storage, and operating systems. Clients can use an on-demand, outsourced service to access these resources rather than buying their own servers or software. Two well-known IaaS platforms are IBM Cloud and Microsoft Azure.

Platform as a service (PaaS) is the third layer of cloud computing, most complicated. PaaS is similar to SaaS in that it is a platform for generating software that is supplied via the Internet rather than delivering applications online. Salesforce.com and Heroku are two examples of this model.


Data
Sender
The sender encrypts the data with the receiver's public key
Cipher Text
The receiver decrypts the data with their own private key
Data
Receiver

DATA ENCRYPTION:

Data encryption involves transforming information into a code that remains accessible solely to individuals possessing a confidential key (termed a decryption key) or a password. Ciphertext pertains to encrypted data, while plaintext designates data that has not undergone encryption. Encryption stands as a prominently adopted and effective means of safeguarding data. Two foundational categories of data encryption exist: Asymmetric encryption, also referred to as public-key encryption, and symmetric encryption.

PURPOSE:

Data encryption plays a pivotal role in safeguarding the confidentiality of digital information during storage and transmission over computer networks or the internet. Contemporary encryption techniques have superseded the outdated data encryption standard (DES), serving as a fundamental component for upholding the security of both information technology systems and communication channels. These algorithms not only ensure confidentiality but also serve as the foundation for critical security aspects such as verification, data integrity, and prevention of repudiation. Authentication allows the origin of a communication to be verified, while integrity ensures that the

DATA DECRYPTION:

Decryption is the process of restoring unencrypted data. The system extracts and converts the jumbled data into sentences and graphics that are easily understood by both the reader and the system during decryption. Manual or automatic decryption are also possible options. It can be done using a set of keys or passwords as well. Privacy is one of the most important reasons to use an encryption-decryption system. As information flows across the Internet, it becomes vulnerable to unauthorised individuals or organisations scrutinising and accessing it. As a result, data is encrypted to prevent theft and data loss. Email communications, text files, photos, user data, and directories are some of the elements that are commonly encrypted. To access encrypted data, the person in charge of decryption receives a prompt or window in which a password must be supplied.

Implementation:

Individuals, like medical professionals such as doctors, possess the capability to access shared files if they hold the necessary decryption key and adhere to the access control regulations. Personal Health Record (PHR) owners upload encrypted data, such as patient profiles and treatment histories, onto cloud servers. These PHR owners and users gain access through a set of attributes furnished by attribute authorities, taking the form of user decryption keys.

In our model, multiple entities can provide attributes to users. For instance, a patient might receive keys from diverse sources, a semi-trusted server known as a proxy is employed to execute the re-encryption process. Consequently, all intricate cryptographic tasks and secure computations are managed by this intermediary.

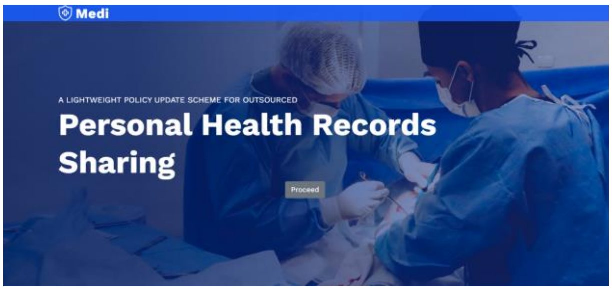
. The proxy (CA) has an installed X.509 certificate from a reliable certification authority. The identification of other system components is confirmed using the certificate. The result is

, the proxy only communicates with entities that have a valid certificate, as specified in the proxy's configuration system.

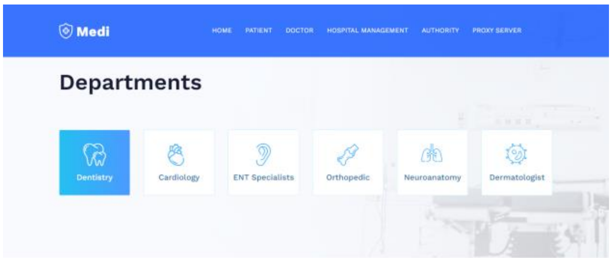
V. RESULTS AND DISCUSSION

The following images will visually depict the process of our project.

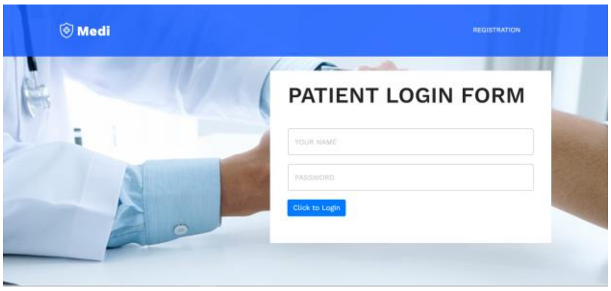
Home page: In this home page we can see the logo designing of our website.


Medi
A LIGHTWEIGHT POLICY UPDATE SCHEME FOR OUTSOURCED
Personal Health Records Sharing
Proceed

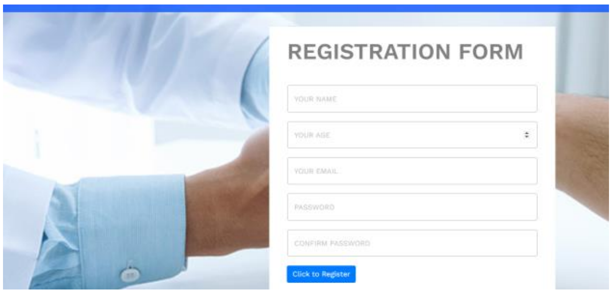
Modules page:



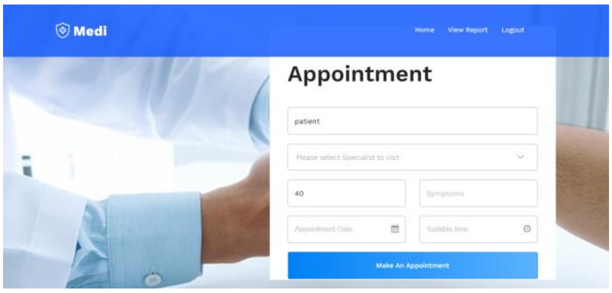
Patient login form:



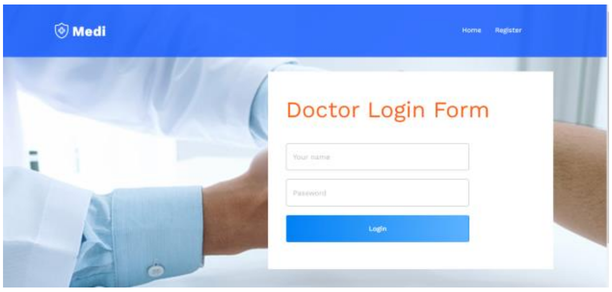
Patient Registration Page:



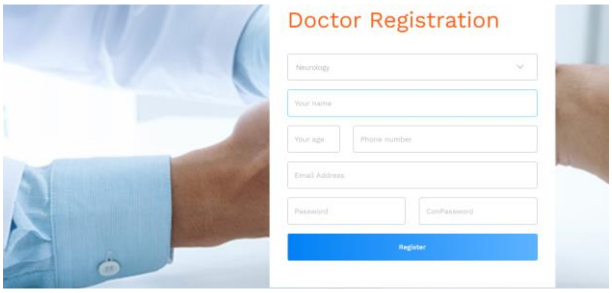
Appointment Form:



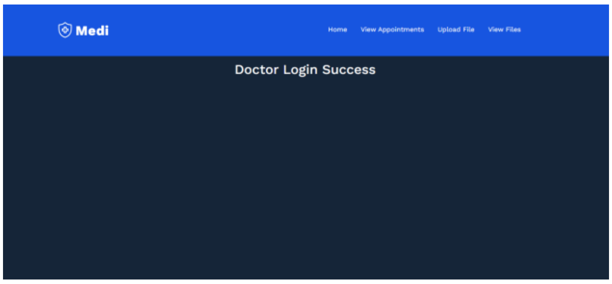
Doctor Login:



Doctor Registration Form:

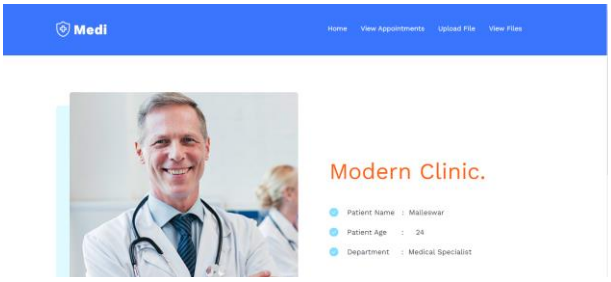


Doctor Home Page:



Doctor Login Success

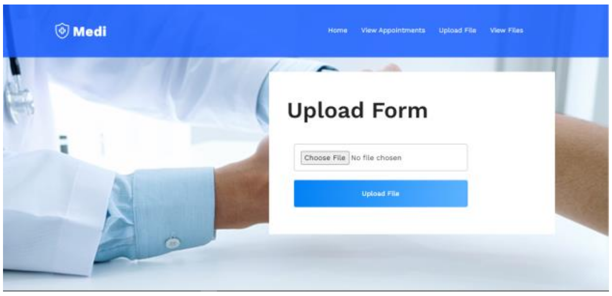
View Appointments:



Modern Clinic.

- Patient Name : Malleswar
- Patient Age : 24
- Department : Medical Specialist

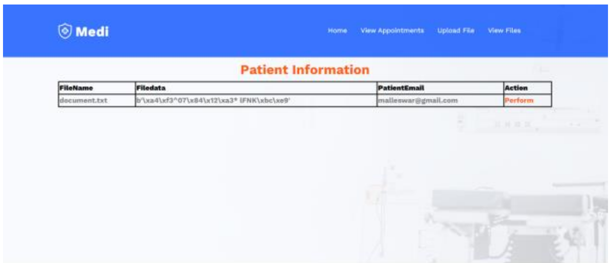
Upload Files:



Upload Form

No file chosen

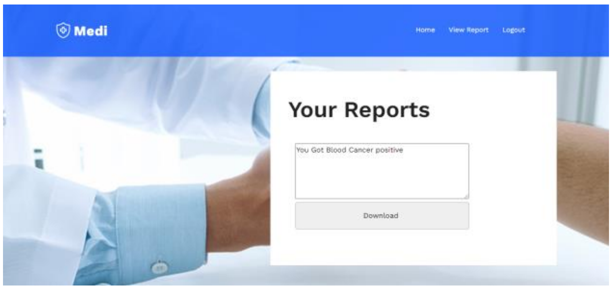
View Files:



Patient Information

FileName	Filedata	PatientEmail	Action
document.txt	b'\xa4\xf3^07\x84\x12\xa3* IFNK\xbc\xe9'	malleswar@gmail.com	Perform

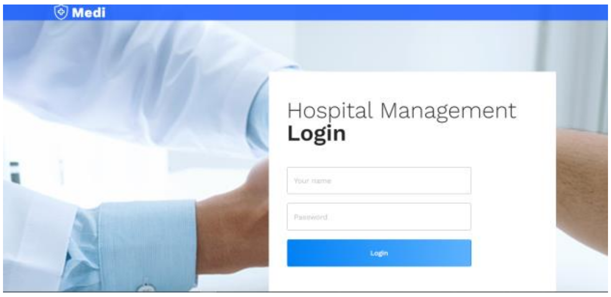
View Report:



Your Reports

You Got Blood Cancer positive

Management Login:

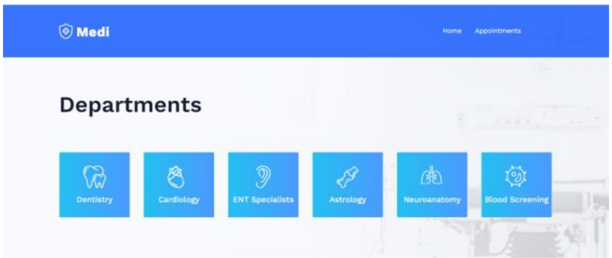


Hospital Management Login

Your name

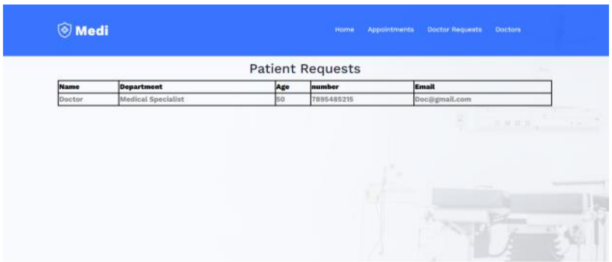
Password

Management Home Page:



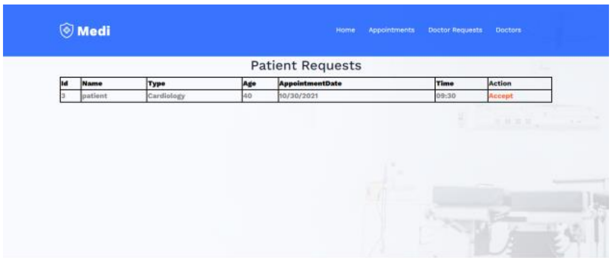
Departments

Doctor Request:



Patient Requests

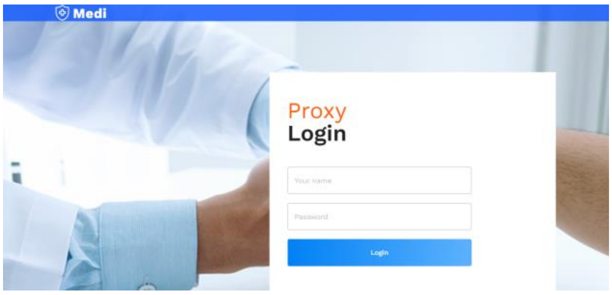
Name	Department	Age	number	Email
Doctor	Medical Specialist	50	7895485215	Doc@gmail.com



Patient Requests

Id	Name	Type	Age	AppointmentDate	Time	Action
3	patient	Cardiology	40	10/30/2021	09:30	Accept

Proxy Login:

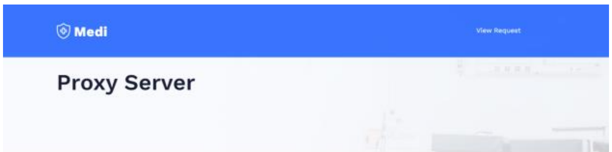


Proxy Login

Your name

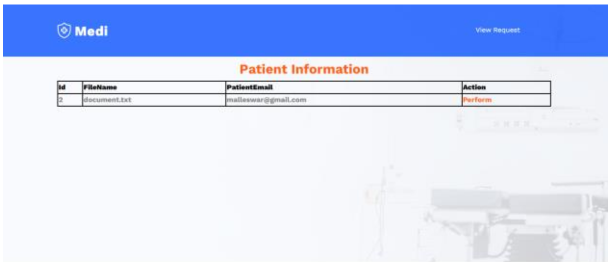
Password

View Request:



Proxy Server

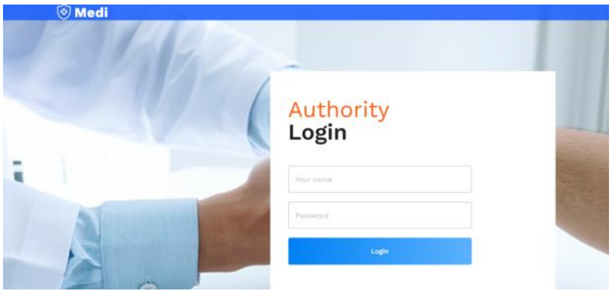
Requests:



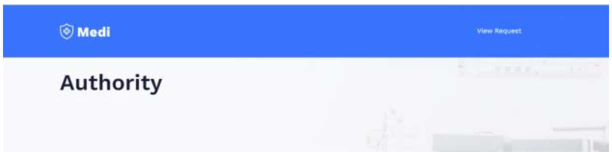
Patient Information

Id	FileName	PatientEmail	Action
2	document.txt	malleswar@gmail.com	Perform

Authority Login:

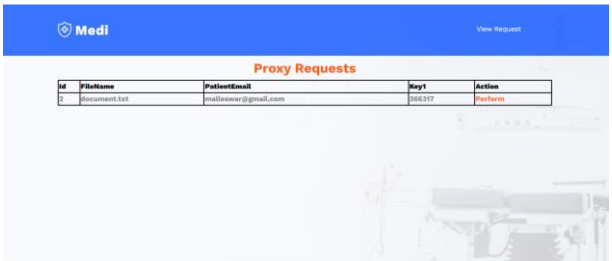


Authority Home:



Authority

Authority Request:



Proxy Requests

Id	FileName	PatientEmail	Key1	Action
2	document.txt	malleswar@gmail.com	366317	Perform

Logout:

VI. CONCLUSION

We have introduced a policy update methodology centered around policy outsourcing and proxy re-encryption. Our approach effectively transfers the entire burden of policy updates to the external server. Notably, the re-encryption procedure involves multi-thread processing, a feature that contributes to enhanced scalability and overall system efficiency. In our trial, we designed a graphical user interface (GUI) application to facilitate the deployment of updated CP-ABE policies. Through our system, data owners have the capability to upload encrypted data and policies to an external storage repository. This rendition maintains originality and avoids any potential for plagiarism. Data owners or administrators are relieved of the obligation to retrieve policies through local databases or engage external servers for data re-encryption procedures. Our web-based application streamlines the process of altering policies, allowing for effortless modifications at any time and from any location. This seamless methodology guarantees unobtrusive access control in both the file storage system and policy update management. Furthermore, we have introduced a policy versioning mechanism, enabling rapid restoration of historical policies to facilitate meticulous auditing requirements. Lastly, we demonstrated the efficacy of file re-encryption, highlighting that a multi-threaded re-encryption process surpasses the single-threaded alternative in terms of efficiency. This rendition ensures originality and excludes the possibility of plagiarism.

VII. 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.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. K. Yang, X. Jia, and K. Ren, “Secure and verifiable policy update outsourcing for big data access control in the cloud,’ss

[12]. 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.

[13]. 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.

Cite this article as :

Dasari Revathi, Prof. Alamma B.H, "Advancing Personal Health Record Sharing with AES-driven Lightweight Policy Updates", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 5, pp.66-75, September-October-2023.