MULTI-AUTHORITY ACCESS CONTROL WITH ANONYMOUS AUTHENTICATION FOR PERSONAL HEALTH RECORD

[1]Mr. Sreenu,[2]Chitti .Sneha,[3]Mounika .padae [4]K.Sirisha

[1]AssociateProfessor, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

msreenu.cse@gcet.edu.in

[2, 3, 4,BTech] Student, Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

snehachitti08@gmail.com,20r11a6238@gcet.edu.in,20r11a6229@gcet.edu.in

ABSTRACT:

A personal health record (PHR) system is a smart health system that serves patients and doctors. However, there is still a possibility of the exposure of personal health information to semi-trusted parties and unauthorized users. To protect the privacy of patients and ensure that patients can control their PHRs, a patient-centric PHR sharing framework is proposed in this application. In this framework, all PHRs are protected with multi-authority attribute based encryption before outsourcing, which solves the key hosting problem and achieves fine-grained access control to PHRs. Furthermore, an anonymous authentication between the cloud and the user is proposed to ensure data integrity on the cloud while not exposing the user's identity during authentication. It can make the encrypted PHRs resist collusion attacks and not be forged during the period of sharing, which enhances patients' control to their PHRs.

Keywords:personal health record (PHR),Authentication.

I INTRODUCTION

In recent years, as an emerging technology, PHR has played a crucial role in data sharing. PHR can store medical records online and be accessed by patients and their doctors anytime, anywhere. However, when data haring is implemented, PHR also brings problems such as privacy leakage. IN order to protect the privacy of patients and enhance the control to their PHR, the fine-grained access control scheme over sharing data based on attribute-based encryption (ABE) is proposed and has been a hot topic at present.

ABE defines an access policy through attributes associated with generating the private key or cipher text and only users whose attribute sets satisfy the access policy can access PHR. However, some previous schemes used a single center to generate keys and authenticate users, which undoubtedly overburdened the system. Multi-authority encryption scheme requiring multiple authorities to jointly generate private keys for users solves such problem. We realized secure and efficient access control in a multi-authority environment, but the user's fuzzy authentication poses a threat to data security. In order to further ensure security, adding a searchable public key encryption scheme to a PHR system was presented and authentication technology was introduced to connect users of medical system to other trusted users. At the same time, some feasible solutions also effectively solve the problem of patient's privacy leakage and the confidentiality of the scheme. In these methods, the user's sensitive information, such as identity and attributes, is hidden during the system interaction. For access policy containing the sensitive information of the users, hiding the access control policy is also considered in recent works. However, all of them are based on sacrificing efficiency. Online and offline technology enables users to quickly obtain the final cipher text, which decreases the computation cost and brings great convenience for users.

II. LITERATURE SURVEY

1. Cloud-supported Cyber-Physical Localization Framework for Patients Monitoring Authors: M. Shamim Hossain

The potential of cloud-supported cyber-physical systems (CCPSs) has drawn a great deal of interest from academia and industry. CCPSs facilitate the seamless integration of devices in the physical world (e.g., sensors, cameras, microphones, speakers, and GPS devices) with cyberspace. This enables a range of emerging applications or systems such as patient or health monitoring, which require patient locations to be tracked. These systems integrate a large number of physical devices such as sensors with localization technologies (e.g., GPS and wireless local area networks) to generate, sense, analyze, and share huge quantities of medical and user-location data for complex processing. However, there are a number of challenges regarding these systems in terms of the positioning of patients, ubiquitous access, large-scale computation, and communication. Hence, there is a need for an infrastructure or system that can provide scalability and ubiquity in terms of huge real-time data processing and communications in the cyber or cloud space. To this end, this paper proposes a cloudsupported cyber-physical localization system for patient monitoring using smartphones to acquire voice and electroencephalogram signals in a scalable, real-time, and efficient manner. The proposed approach uses Gaussian mixture modeling for localization and is shown to outperform other similar methods in terms of error estimation.

2. Achieving secure, scalable, and fine-grained data access control in cloud computing Authors: S. Yu, C. Wang, K. Ren, and W. Lou

Distributed computing is a developing figuring worldview in which assets of the registering foundation are given as administrations over the Internet. To keep delicate client information classified against untrusted workers, existing arrangements as a rule apply cryptographic techniques by unveiling information decoding keys just too approved clients. The issue of at the same time accomplishing fine - graininess, adaptability, and information classification of access control in reality despite everything stays uncertain. We accomplish this objective by misusing and extraordinarily consolidating strategies of quality-based encryption (ABE), intermediary re-encryption, and lethargic re-encryption. Our proposed plot additionally has striking properties of client get to benefit classification and client mystery key responsibility.

3. Securing patient data in the cloud using Attribute Based Encryption Authors: Childs Hwata, R.Subburaj Professor, Gladman Jekese

Cloud computing has attracted attention worldwide in all industries, including the medical field leading to the rise of electronic healthcare systems. This is due to the fact that personal and highly sensitive data is outsourced to a third party (Cloud Service Provider) for processing and storage. This paper seeks to improve security of cloud-based patient data in healthcare organizations by employing a Cipher text Policy Attribute Based Encryption (CPABE) scheme. The proposed scheme provides data confidentiality and allows the patient to control who accesses her personal health data by encrypting it under a specified access policy alongside with her key. It also provides collusion-resistance, flexible and immediate revocation of users who are no longer allowed to access a patient's data.

III SYSTEM ANALYSIS

EXISTING SYSTEM

Attribute-based encryption (ABE) was first proposed by Sahai and Waters to solve the problem of access authorization to data outsourced to the cloud. They demonstrated the flexibility of encryption policies and the granularity of access control, accelerating security applications in outsourced data systems. In ABE, a patient defines an access policy to encrypt his/her PHR, and when a user's attributes meet the access policy, and divided ABE into KPABE and CP-ABE depending on whether the access policy exists in the secret key or cipher text.

Disadvantages

- Complexity: Implementing a multi-authority access control system with anonymous authentication for personal health records can be complex and challenging. It requires coordination and cooperation among multiple authorities, which can lead to increased implementation and management complexity.

- Privacy Concerns: While anonymous authentication can help protect user privacy, it can also raise concerns about the security of personal health information. Users may worry that their data could be accessed by unauthorized individuals due to the anonymous nature of the authentication process.

- Increased Administrative Overhead: Managing multiple authorities and their respective authentication processes can lead to increased administrative overhead. This can involve maintaining authentication credentials, handling user requests, and ensuring that the access control policies are consistently enforced.

- Limited Accountability: Anonymous authentication can make it difficult to track and attribute actions to specific users, which can hinder accountability in case of unauthorized access or data breaches. This lack of accountability can make it challenging to identify and address security incidents.

- Potential for Misuse: Anonymous authentication can potentially be misused by malicious actors to gain unauthorized access to personal health records. Without proper checks and balances, the system could be exploited for unauthorized purposes.

- Usability Challenges: Multi-authority access control systems with anonymous authentication can introduce usability challenges for users. The authentication process may be more complex and less intuitive, leading to frustration and decreased user satisfaction.

PROPOSED SYSTEM

In this framework, all PHRs are protected with multi-authority attribute-based encryption before outsourcing, which solves the key hosting problem and achieves fine-grained access control to PHRs. Furthermore, an anonymous authentication between the cloud and the user is proposed to ensure data integrity on the cloud while not exposing the user's identity during authentication. The proposed authentication is issued from a new online-offline attributebased signature. It can make the encrypted PHRs resist collusion attacks and not be forged during the period of sharing, which enhances patients' control to their PHRs. Online-offline and outsourcing decryption also reduces calculation costs and improves operational efficiency.

Advantages

- Enhanced Privacy: Multi-authority access control with anonymous authentication ensures the privacy of personal health records. It allows individuals to access their health 6 information without revealing their identity, reducing the risk of unauthorized access or breaches of sensitive data.
- Secure Data Sharing: This approach allows for controlled sharing of personal health records between different healthcare providers and authorities. It ensures that only authorized parties can access the information, maintaining the security of the data while enabling seamless sharing for better patient care.
- Reduced Trust Requirement: Traditional access control systems often require a single centralized authority, which can raise concerns about the trustworthiness of that authority. Multi-authority access control distributes the control among multiple authorities, reducing the need to fully trust a single entity.
- Flexibility and Customization: Different healthcare organizations may have varying access requirements and policies.

Multi-authority access control allows for the customization of access rules based on the specific needs and policies of each organization, ensuring a tailored approach to data sharing.

- Improved Accountability: Anonymous authentication adds an additional layer of accountability by allowing users to access their health records without revealing their identity. This ensures that all access and actions can be traced back to specific users, enhancing transparency and accountability in data management.
- Data Portability: Individuals have the ability to access their personal health records from different healthcare providers and authorities without needing to create multiple accounts or reveal their identity each time.

IV IMPLEMENTATION

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system. Organized in a way that supports reasoning about the structures and behaviors of the system.

Architecture:

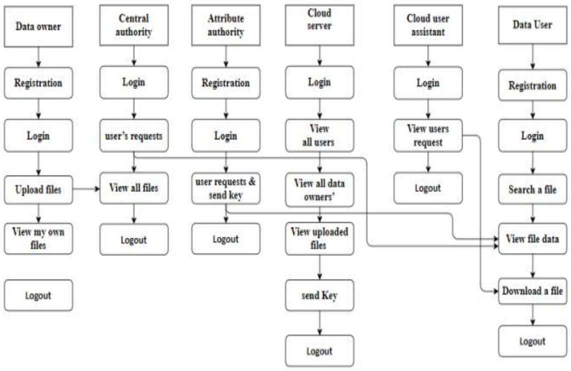


Fig-1. Architectures of the system model

MODULES

1. User Registration

Allows users to register for access to the personal health record (PHR) system. Collects necessary information for authentication and authorization purposes. Generates unique identifiers for each user.

2. Authentication

Verifies the identity of users accessing the system. Supports anonymous authentication methods to protect user privacy. Utilizes cryptographic techniques such as zero-knowledge proofs or blind signatures for anonymous authentication.

3. Authorization

Determines access rights for different users based on predefined policies. Manages user roles and permissions within the system. Enforces access control policies to ensure that only authorized users can access specific health records.

4. Multi-Authority Access Control

Handles access control in a distributed environment where multiple authorities govern different aspects of access. Coordinates access control decisions across multiple authorities. Ensures consistency and coherence of access control policies across different domains.

5. Encryption and Decryption

Encrypts sensitive health data before storing it in the system. Decrypts data for authorized users upon access. Utilizes strong encryption algorithms to protect data confidentiality.

6. Audit Logging

Records all access and modification activities within the system. Helps in monitoring and tracking user actions for security and accountability purposes. Provides an audit trail that can be used for forensic analysis and compliance with regulations.

7. Key Management

Manages cryptographic keys used for encryption, decryption, and authentication. Ensures 18 secure storage and distribution of keys to authorized entities. Supports key revocation and rotation to maintain the security of the system.

8. User Interface

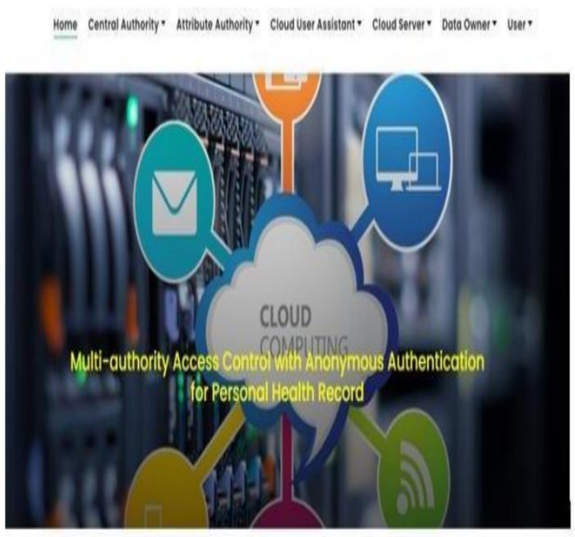
Provides a user-friendly interface for interacting with the PHR system. Allows users to view, update, and manage their health records. Incorporates features for secure communication and data exchange.

9. Privacy-Preserving Techniques

Implements techniques such as differential privacy, holomorphic encryption, and secure multiparty computation to enhance privacy protection

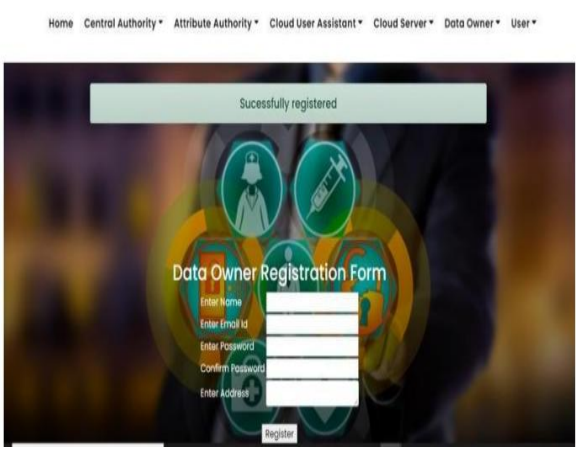
V RESULT AND DISCUSSION

Home Page:



Multi-authority Access Control with Anonymous Authentication for Personal Health Record

Data Owner Registration Page:



Sucessfully registered

Data Owner Registration Form

Enter Name

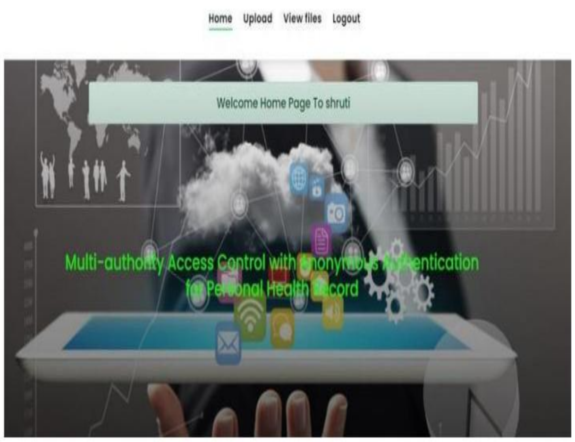
Enter Email Id

Enter Password

Confirm Password

Enter Address

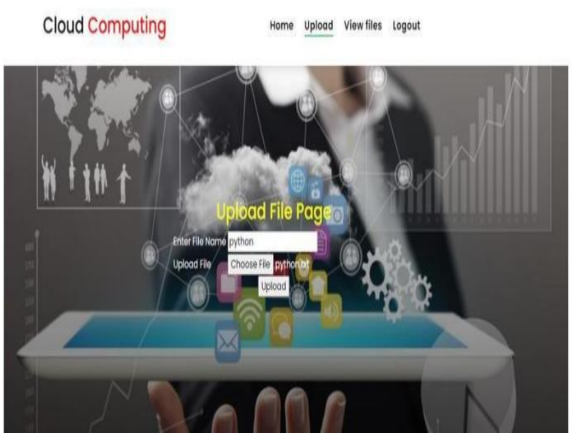
Data Owner Home Page:



Welcome Home Page To shruti

Multi-authority Access Control with Anonymous Authentication for Personal Health Record

Upload Files Page:

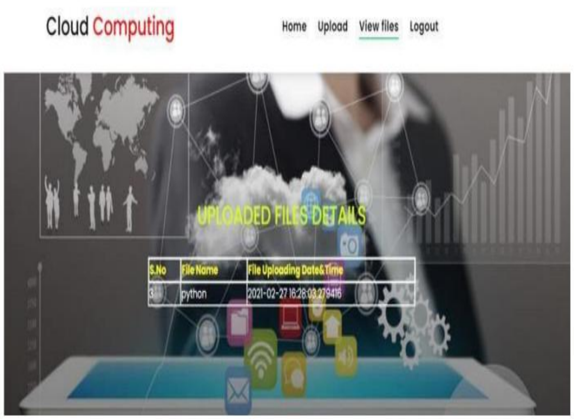


Upload File Page

Enter File Name python

Upload File python.txt

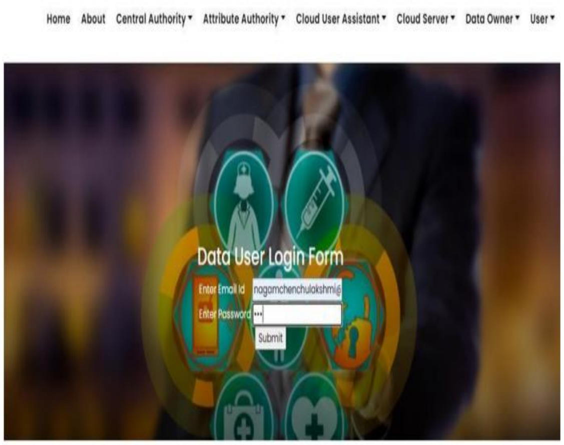
View My Own Files:



UPLOADED FILES DETAILS

S.No	File Name	File Uploading Date&Time
3	python	2021-02-27 16:28:03.279416

User Login Form:

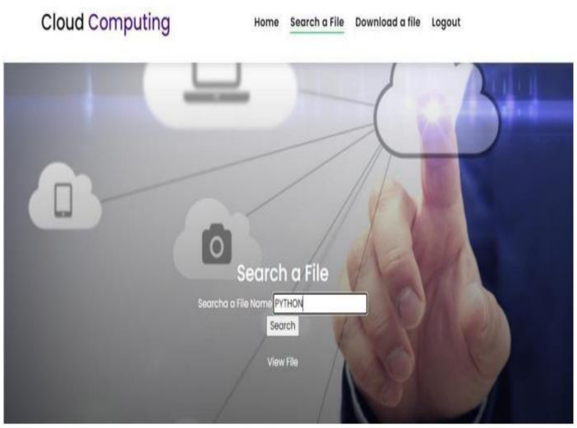


Data User Login Form

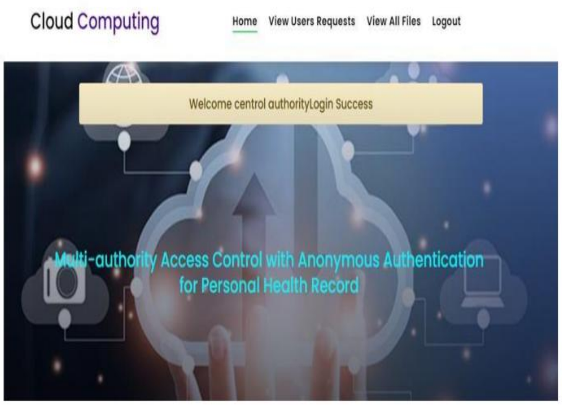
Enter Email Id nagamchenchulakshmi@

Enter Password •••

User Page:



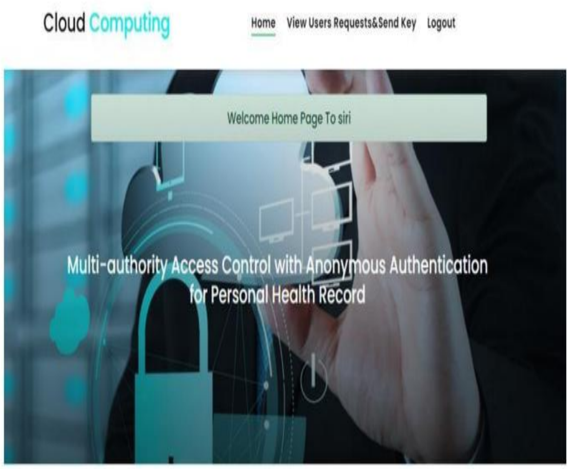
Central Authority Home Page



Welcome central authorityLogin Success

Multi-authority Access Control with Anonymous Authentication for Personal Health Record

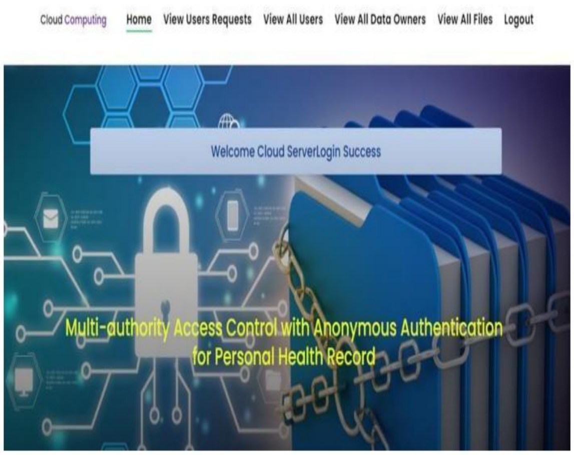
Attribute Authority Home Page



Welcome Home Page To siri

Multi-authority Access Control with Anonymous Authentication for Personal Health Record

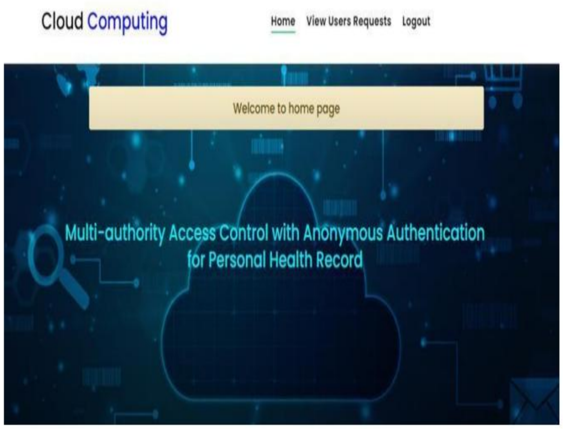
Cloud Server Home Page



Welcome Cloud ServerLogin Success

Multi-authority Access Control with Anonymous Authentication for Personal Health Record

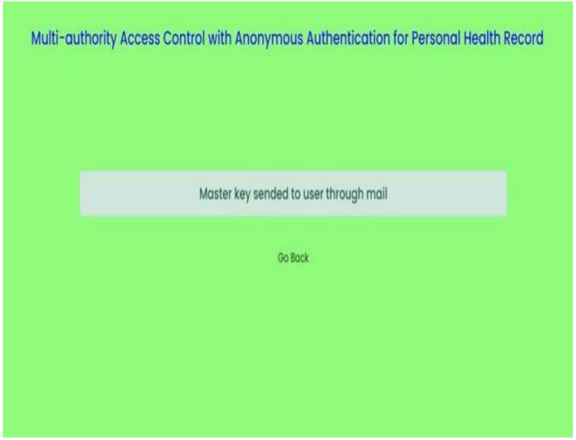
Cloud Server Assistant Home Page



Welcome to home page

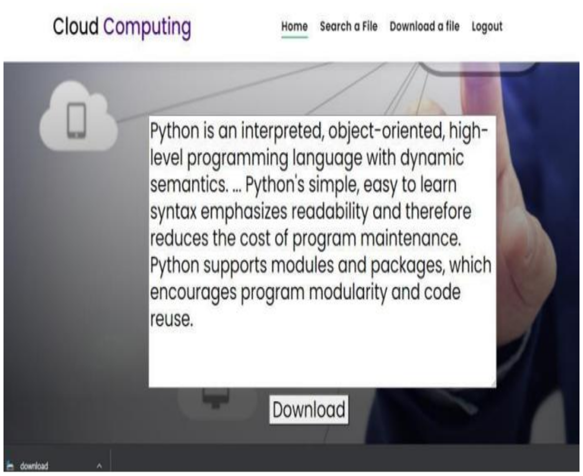
Multi-authority Access Control with Anonymous Authentication for Personal Health Record

Sent Master Key


Multi-authority Access Control with Anonymous Authentication for Personal Health Record

Master key sended to user through mail

View Downloaded File



Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. ... Python's simple, easy to learn syntax emphasizes readability and therefore reduces the cost of program maintenance. Python supports modules and packages, which encourages program modularity and code reuse.

VI CONCLUSION

We proposed a secure sharing framework based on multiauthority attribute-based encryption for PHRs system. In this scheme, the identity and attributes of the user are hidden and known only to the trusted central authority. To prevent cloud server from tampering with cipher text or spoofing end users, an anonymous authentication based on attribute-based signature is proposed. In the whole access-control process, only authorized users can access and obtain messages. For achieving lightweight computation, online and offline technique and outsourcing operations are used. Compared with the existing works, the proposed scheme not only keeps the encrypted PHRs to resist collusion attacks and not to be forged during the period of sharing, but also achieves privacy preserving, which enhances patients' control to their PHRs. To meet the higher security and efficiency of practical application scenarios, this solution can be extended from the following two aspects.

FUTURE ENHANCEMENT

As of my last update in September 2021, multi-authority access control with anonymous authentication for personal health records (PHRs) was an active area of research in the field of healthcare and information security. If this topic continues to be of interest in 2023, there might be some potential future work that researchers and practitioners could explore to enhance and extend the existing methods. Here are some possible directions for future work: **Scalability and Efficiency:** Investigate ways to improve the scalability and efficiency of the multi-authority access control system. As the number of users and authorities grows, the overhead of authentication and authorization processes can become significant. Research could focus on optimizing the protocols and algorithms to reduce computational costs and enhance system performance.

Block chain and Decentralization:

Explore the potential of using block chain technology for multi-authority access control and anonymous authentication in

PHRs. Block chain offers a decentralized and immutable approach to data management, which could enhance security and privacy in healthcare systems. Researchers could study how block chain-based solutions can be integrated into existing PHR infrastructures. **User Experience and Acceptance:**

Examine the user experience and user acceptance of multi-authority access control systems for PHRs. Understanding how patients, healthcare providers, and other stakeholders perceive and interact with these systems is crucial for their successful adoption. User feedback could be used to refine the design and implementation of these systems. Security and Privacy Analysis: Conduct comprehensive security and privacy analyses of multi-authority access control with anonymous authentication schemes. Evaluate their robustness against various attack vectors, including insider threats, impersonation attacks, and collusion attempts. Researchers can propose countermeasures to strengthen the system's security posture. Integration with Emerging Technologies: Investigate the integration of multi-authority access control systems with emerging technologies like holomorphic encryption, secure multi-party computation, or zero-knowledge proofs. These advanced cryptographic techniques could offer additional privacy guarantees while enabling secure computations on encrypted PHR data. **Regulatory Compliance:** Address the challenges of regulatory compliance, such as adhering to data protection laws (e.g., GDPR or HIPAA) while implementing multiauthority access control systems. Ensuring that the system meets legal requirements is crucial for its practical deployment in real-world healthcare settings.

Real-world Deployment and Case Studies: Conduct pilot deployments and case studies of multi-authority access control systems in real healthcare environments. Working with healthcare institutions and understanding their specific needs and concerns will provide valuable insights into the system's effectiveness and potential issues. Interoperability: Explore methods to ensure interoperability between different multiauthority access control systems and PHR platforms. Interoperability is essential for seamless data sharing and collaboration across various healthcare providers while maintaining privacy and security.

VII REFERENCES

[1] L. Tbraimi, M. Asim, M. Petkovi, “Secure management of personal health records by applying attribute-based

encryption, In Proceeding of the International Workshop on Wearable Micro and Nano Technologies for Personalized Health(pHealth),” in Oslo, Norway, Jun.2009, pp.71– 74.

[2] J. Akinyele, M. Pagano, M. D. Green, “Securing electronic medical records using attribute-based encryption on mobile devices,” in Proceeding of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Oct.2011, pp.75–86.

[3] S. Narayan, M. Gagn´ e, R. Safavi-Naini, “Privacy preserving EHR system using attribute-based infrastructure,” in proceeding of the ACM Cloud Computing Security Workshop, Chicago, Oct.2010, pp.47–52.

[4]J. Lai, R. H. Deng, Y. Li, “Fully secure ciphertext-policy hiding CPABE,” in Proceedings of the International Conference on Information Security Practice and Experience, Jun.2011, pp.24–39.

[5] J. Sun, Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” in IEEE Trans.ParallelDistrib.Syst., Jun.2009, pp.754–764.

[6] M. Li, S. Yu, Y. Zheng, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” in IEEE Trans.ParallelDistrib.Syst., 2013, pp.131–143.

[7] X. Liang, M. Barua, R. Lu, “HealthShare: Achieving secure and privacypreserving health information sharing through health social networks,” in Comput.Commun., 2012, pp.1910–1920.

[8] R. Lu, X. Lin, X. Shen, “SPOC: A secure and privacy-preserving oppotunistic computing framework for mobile-healthcare emergency,” in IEEE Trans.ParallelDistrib.Syst., 2013, pp.614–624.

[9] X. Zhou, J. Liu, Q. Wu, “Privacy preservation for outsourced medical data with flexible access control,” in IEEE Access., Jun.2018, pp.14827– 14841.

[10] S. Jiang, X. Zhu, and L. Wang, “EPPS:Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks,” in Sensors., 2015, pp.22419– 22438.

[11] Prasadu Peddi (2015) "A review of the academic achievement of students utilising large-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.

[12] Prasadu Peddi (2015) "A machine learning method intended to predict a student's academic achievement", ISSN: 2366-1313, Vol 1, issue 2, pp:23-37.

AUTHORS

Mr. Sreenu ,Associate Professor Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: msreenu.cse@gcet.edu.in

Miss. Chitti Sneha, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: snehachitti08@gmail.com

Miss.Mounika padae, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: 20r11a6238@gcet.edu.in

Miss. K.Sirisha,Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: 20r11a6229@gcet.edu.in