Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

SECURE IDENTITY-BASED DATA SHARING AND PROFILE MATCHING FOR MOBILE HEALTHCARE SOCIAL NETWORKS IN CLOUD COMPUTING

Mr .K. Pavan Kumar (Guide), , Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam**,** India
P. Sharun, Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam**,** India
R. Trinadha Rao, Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam**,** India
G. Uday, Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam**,** India
P. Chaitanya, (4th year B.Tech Students) , Computer Science & Engineering Department, Raghu Engineering College, Visakhapatnam**,** India

ABSTRACT
Social media and cloud computing are revolutionizing healthcare by enabling affordable, real-time data sharing. However, given that health information is regarded as extremely sensitive, data security issues are one of the primary barriers to the widespread adoption of mobile healthcare social networks (MHSN). We present a secure profile matching and data sharing scheme for cloud computing MHSN in this paper. Patients can securely and effectively share their encrypted health records with a group of doctors by outsourcing them to cloud storage using identity-based broadcast encryption (IBBE) technique. Social media and cloud computing are revolutionizing healthcare by enabling affordable, real-time data sharing. However, given that health information is regarded as extremely sensitive, data security issues are one of the primary barriers to the widespread adoption of mobile healthcare social networks (MHSN). We present a secure profile matching and data sharing scheme for cloud computing MHSN in this paper. Patients can securely and effectively share their encrypted health records with a group of doctors by outsourcing them to cloud storage using identity-based broadcast encryption (IBBE) technique. Next, we present an attribute-based conditional data re-encryption construction that allows doctors to authorize the cloud platform to convert their data if they meet the pre-defined conditions in the ciphertext.

KEYWORDS:
User profile matching, data privacy protection, ElGamal encryption, Pallier encryption, homomorphic encryption.

1. INTRODUCTION
1 INTRODUCTION
Innovatively combining mobile devices and mobile communication technologies, mobile healthcare offers essential health information, routine care enhancements, possible prevention of infectious diseases, health interventions, etc. The use of cutting-edge cloud computing technology in the domains of mobile healthcare is spreading more and more. The electronic health record (EHR) can be sent over the network to the cloud service provider (CSP) for remote storage by using a mobile healthcare system. In order to provide medical care in real time, the healthcare providers can also read it from an end device or access it remotely using a mobile device. Since social media is an extension of the relationship between a healthcare provider and patient, people prefer to share and spread healthcare information through these platforms.
The creation and deployment of a Secure Identity-based Data Sharing and Profile Matching system for MHSNs is the main goal of this project. The project intends to create a secure framework for data sharing by utilizing sophisticated identity-based mechanisms to limit access to authorized users only. Concurrently, the creation of effective algorithms for profile matching aims to improve the caliber of

user connections in the network.

The project includes creating, designing, and putting into use a safe framework for sharing identity-based data. To protect health data, this also involves integrating authentication and encryption protocols. In order to improve user connections based on health characteristics and provide a more relevant and personalized user experience, profile matching algorithms will also be developed.

2. LITERATURE SURVEY AND RELATED WORK

2.1 Introduction to Literature Survey:

Healthcare is undergoing a paradigm shift thanks to Mobile Healthcare Social Networks (MHSNs), which provide a vibrant forum for people to exchange health information, have conversations, and get support. But resolving privacy issues related to sharing health data and improving the relevancy of user connections through profile matching are critical to these networks' success. In order to better understand secure identity-based data sharing and profile matching for MHSNs, this literature review examines current studies and technological advancements in the field.

2.2 Literature Survey:

Survey on "Attribute-based encryption for scalable and secure sharing of personal health records in cloud computing":

An emerging framework for exchanging health information is the Personal Health Record (PHR), which is frequently kept on cloud servers. However, there are still a number of privacy issues since unauthorized parties may find out about private health information. Encrypting PHRs before storing them on the cloud is one way to ensure that patients retain control over their own PHRs. However, concerns like privacy risks, effective key management, adaptable access, and effective user management continue to be major obstacles in the way of improving cryptographically enforced data access control. In this study, we create a framework and a method for managing PHR data access.

2..2.2 "Lightweight, sharable, and traceable secure mobile health system" survey results:

A new patient-centered paradigm known as mobile health (mHealth) enables the real-time collection of patient data using wearable sensors, aggregates and encrypts that data on mobile devices, and then uploads that encrypted data to the cloud so that medical professionals and researchers can access and store it. Sharing encrypted data in an effective and scalable manner has proven to be a very difficult problem. In this study, we present a secure mobile health system that is lightweight, scalable, and traceable (LiST). Patient data are encrypted all the way from the patient's mobile device to the data users. Effective keyword search and fine-grained access management of encrypted data are made possible by LiST, which also facilitates the tracking of traitors who sell their search and access rights.

2.2.3 Survey on “Proxy re-encryption systems for identity-based encryption”:

A proxy re-encryption system allows the proxy to transform ciphertexts encrypted under Alice’s public key into the different ciphertexts that can be decrypted by Bob’s secret key. In this paper, we propose new proxy re-encryption systems; one for the transformation from ciphertexts encrypted under a traditional certificate-based public key into the ciphertexts that can be decrypted by a secret key for Identity-Based Encryption, and the other one for the transformation from ciphertexts encrypted in IBE manner into the different ciphertexts that can be decrypted by the other secret key for the IBE.

2.2.4 A survey titled "Secure chosen-ciphertext encryption using conditional proxy re-encryption"

A proxy, approved by Alice, can change a ciphertext intended for Alice into a ciphertext intended for Bob in a proxy re-encryption (PRE) system [4] without viewing the underlying plaintext. There are numerous real-world uses for PRE that call for delegation. It cannot, however, handle situations where a more detailed delegation is required. We present the idea of conditional proxy re-encryption (C-PRE), which circumvents the drawbacks of current PRE systems by allowing Bob to decrypt only cipher text that satisfies a particular criteria defined by Alice. We present an effective C-PRE scheme and describe its security model. The chosen ciphertext security is validated using the 3-

quotient bilinear Diffie-Hellman assumption. We expand the construction even farther.
An overview of "Attribute-based encryption using ciphertext policies":

A user should only be granted access to data in a number of distributed systems if they meet specific requirements or possess particular qualities. As things stand, the only way to enforce these requirements is to use a trusted server to handle access control and store data. However, the confidentiality of the data will be jeopardized if any server hosting the data is compromised. In this research, we propose a new approach, which we name Ciphertext-Policy Attribute-Based Encryption, to achieve sophisticated access control on encrypted data. Even if the storage server is unreliable, encrypted data may be kept private with our methods since they are safe from collusion assaults. In the past, attribute-based encryption schemes described the

3 Implementation Study & Algorithm

3.1 EXISTING Methodologies

On the other hand, the main challenges to MHSN application are data security concerns. Health information, including information about medications and treatments, is, as we all know, regarded as extremely sensitive. The patients will not have direct control over the hardware or software platform used to store the data if it is outsourced to the CSP. Patients could experience severe medical information leaks from the cloud if this isn't carefully thought out. For instance, millions of electronic health records have been hacked lately. Therefore, it is imperative that the electronic health records be stored in an encrypted format. The data is secure and private even in the event that the CSP is compromised or not trusted. The encrypted records should be accessible and exchanged in a suitable manner at the same time.

3.2 PROPOSED Methodology

Our proposal for MHSN is a secure identity-based data sharing scheme that enables patients to securely and effectively communicate their encrypted health records with a group of doctors by outsourcing the records to CSP using the IBBE approach. We describe an attribute-based conditional data re-encryption design that allows physicians to grant permission to the CSP to re-encrypt the ciphertext for specialists without disclosing any private information, provided they meet the pre-defined conditions in the ciphertext. Our MHSN profile matching system, which is based on the IBE with equality test (IBEET), is effective in helping patients meet friends while protecting their privacy. It also allows for flexible authorization on encrypted health records while fending against keyword guessing attacks.

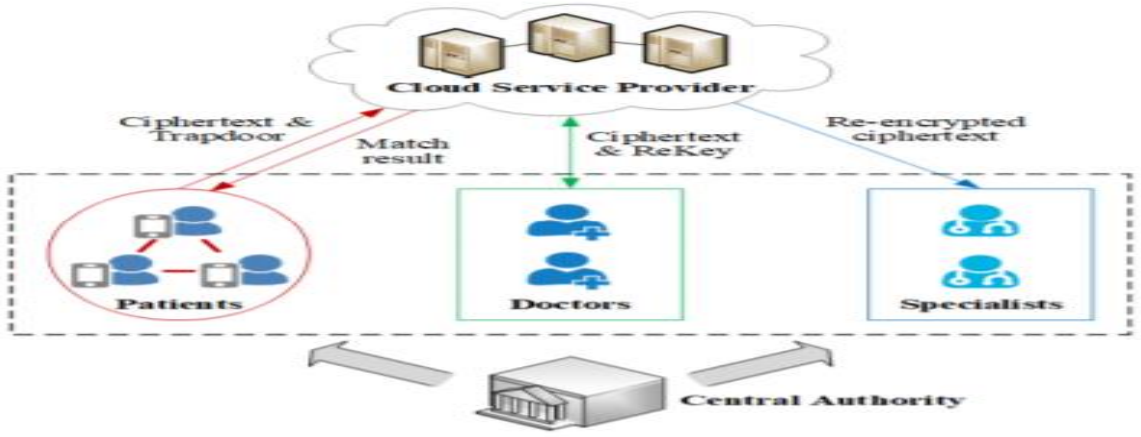


Fig 1 :- SYSTEM ARCHITECTURE

3.3 Identity Based Encryption Algorithm

Identity-Based Encryption (IBE) is a type of public-key encryption where a user's identity, such as an email address or a username, can be used as a public key. Here's a basic step-by-step explanation of how an IBE algorithm typically works:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

1. Setup Phase:
   - Master Key Generation: A trusted authority (referred to as the Key Generation Center or KGC) generates a master key pair. This consists of a master private key (usually a large random number) and a master public key.
2. Key Extraction:
   - User Registration: When a user wants to participate in the system, they register with the KGC. During registration, the KGC extracts the user's private key based on their identity and the master private key. This process usually involves some sort of authentication to verify the user's identity.
   - **Private Key Distribution**: The KGC then securely sends the user their private key.
3. Encryption:
   - Key Derivation: To encrypt a message for a particular user, the sender uses the recipient's identity to derive their public key from the master public key. This derivation process typically involves a one-way hash function or some other cryptographic method.
   - Message Encryption: The sender then encrypts the message using the derived public key. This can be done using standard symmetric or asymmetric encryption algorithms.
4. Decryption:
   - **Private Key Retrieval**: When the recipient wants to decrypt the message, they present their identity to the KGC.
   - Private Key Generation: Using the recipient's identity and the master private key, the KGC generates the recipient's private key on the fly and sends it securely to the recipient.
   - Message Decryption: The recipient then decrypts the message using their private key.

It's worth noting that there are variations of IBE schemes, and the exact steps may differ depending on the specific algorithm being used. Additionally, there are security considerations, such as key management and protection against various attacks, that need to be addressed in any practical implementation of an IBE system.

4. RESULTS AND DISCUSSION SCREEN SHOTS

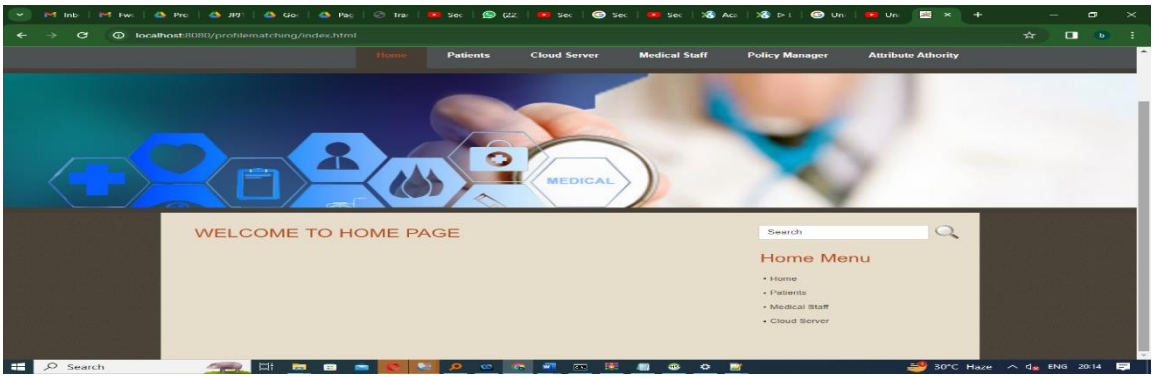
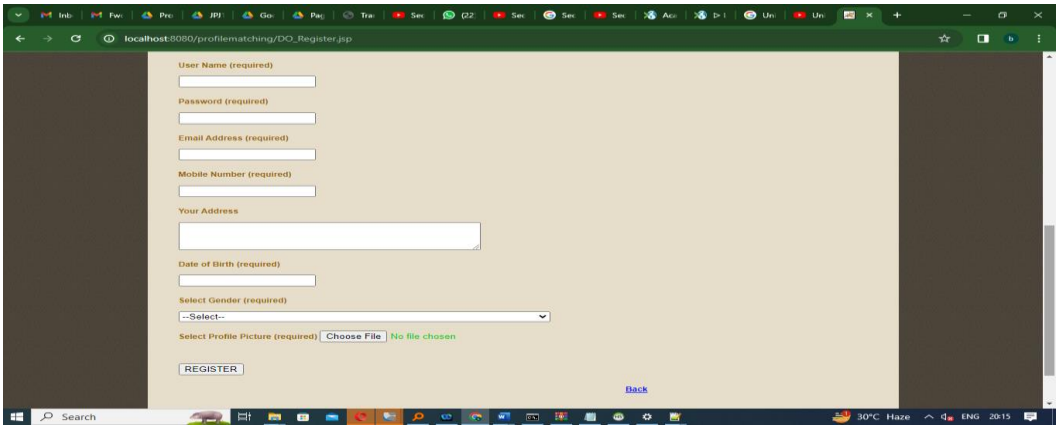


Fig 2 Home Page



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Fig 3 Patient Registration Form

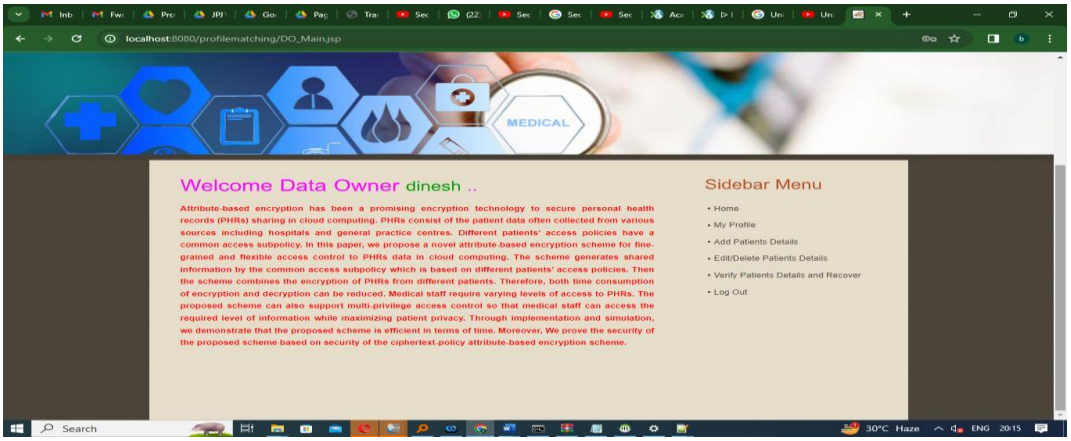


Fig4 Patient Home Page

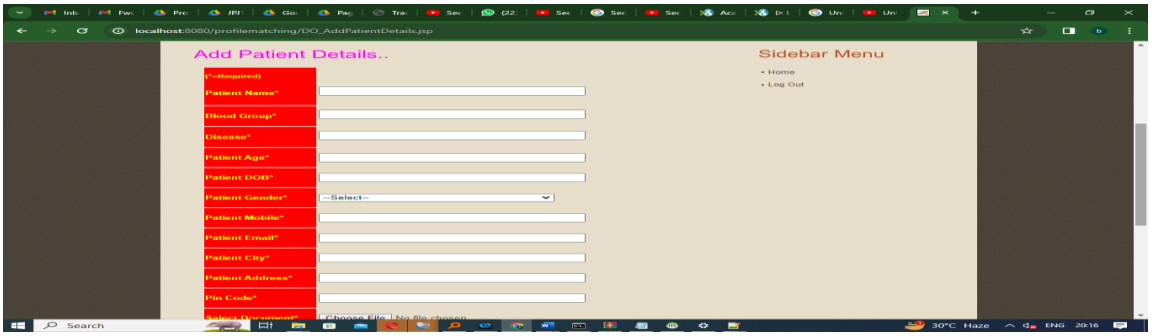


Fig 5 Adding Patient Details

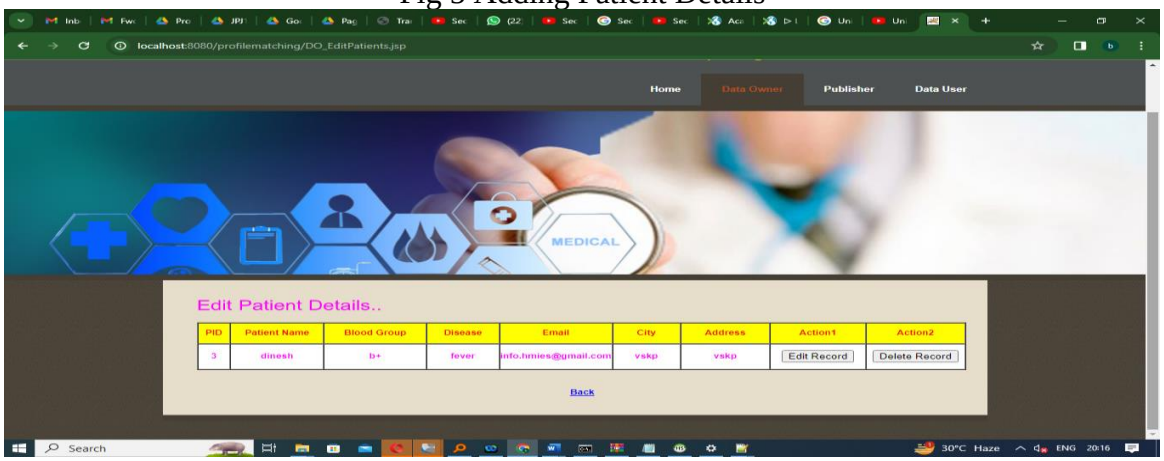
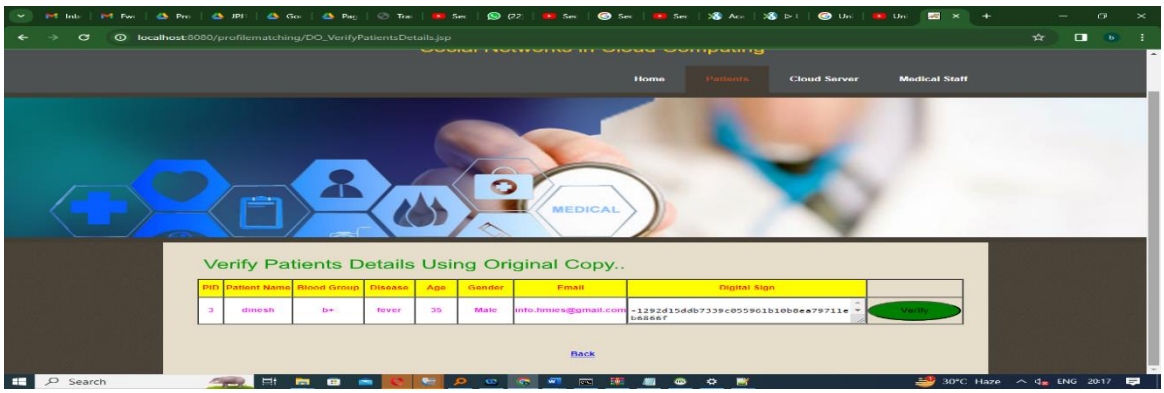


Fig 6 Patient Details Edit Page



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Fig 7 Patient Details Verification Page

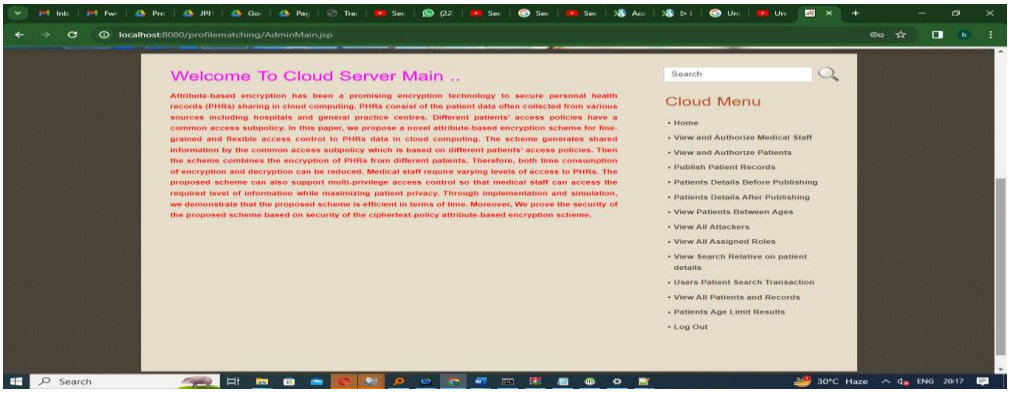


Fig 8 Coud Home Page

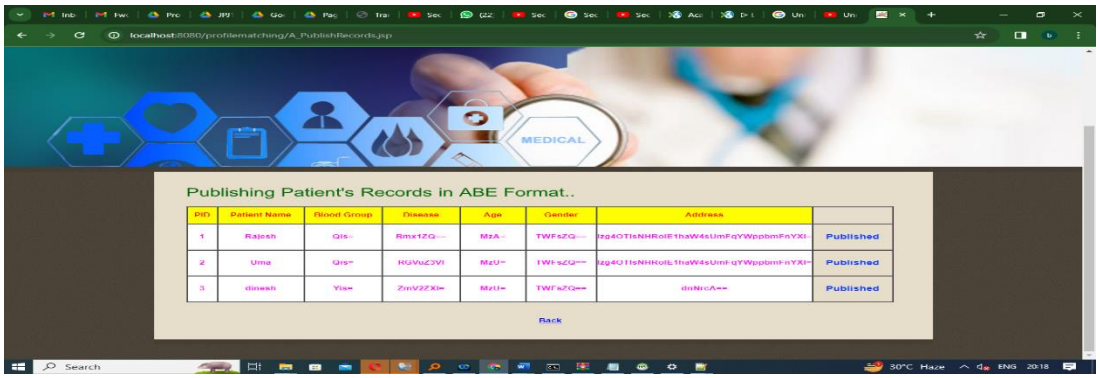


Fig 9 Publishing Patient Records

Fig 10 Patient Details After Publishing

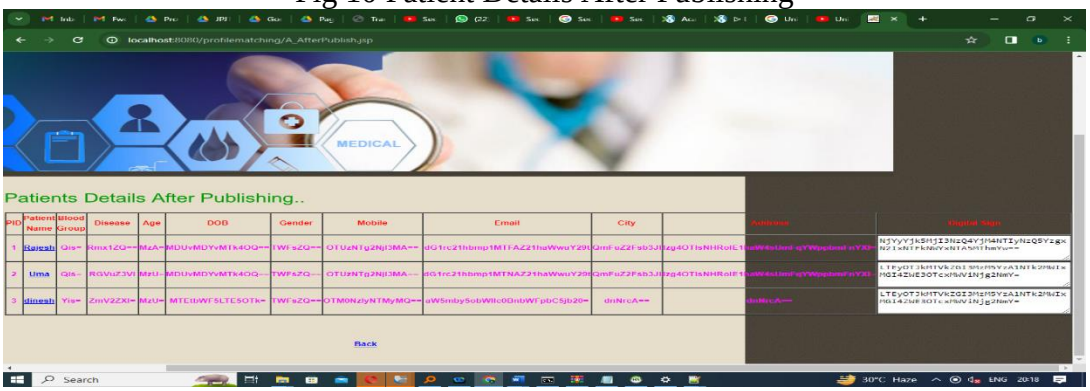


Fig 11 :- Data Encrypted using IBE Algorithm

Fig 12 Searching Patient Details and Profile Matching

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

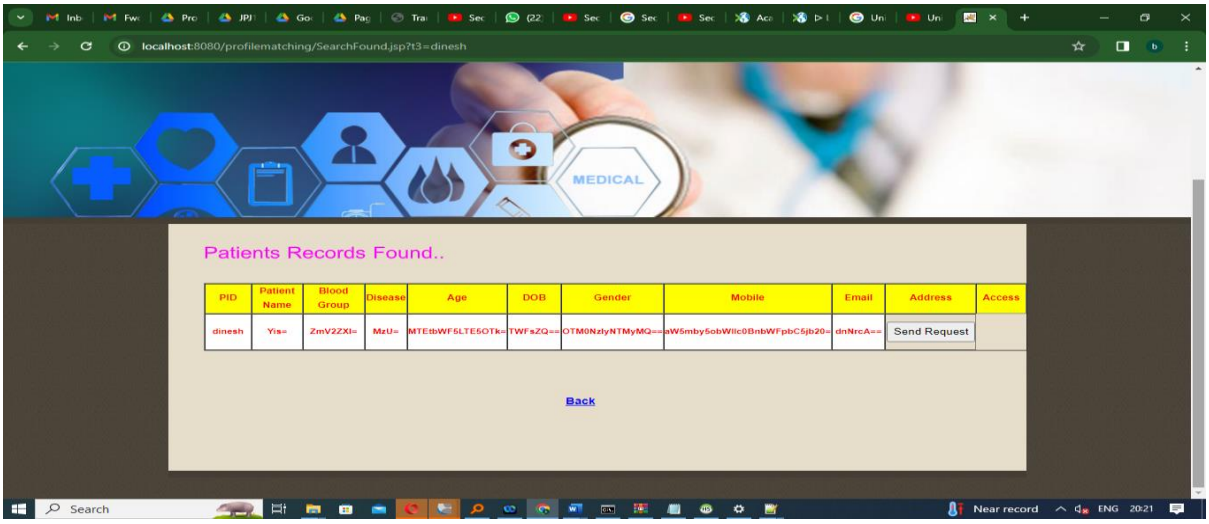


Fig 13 Searching Patient Profile Data

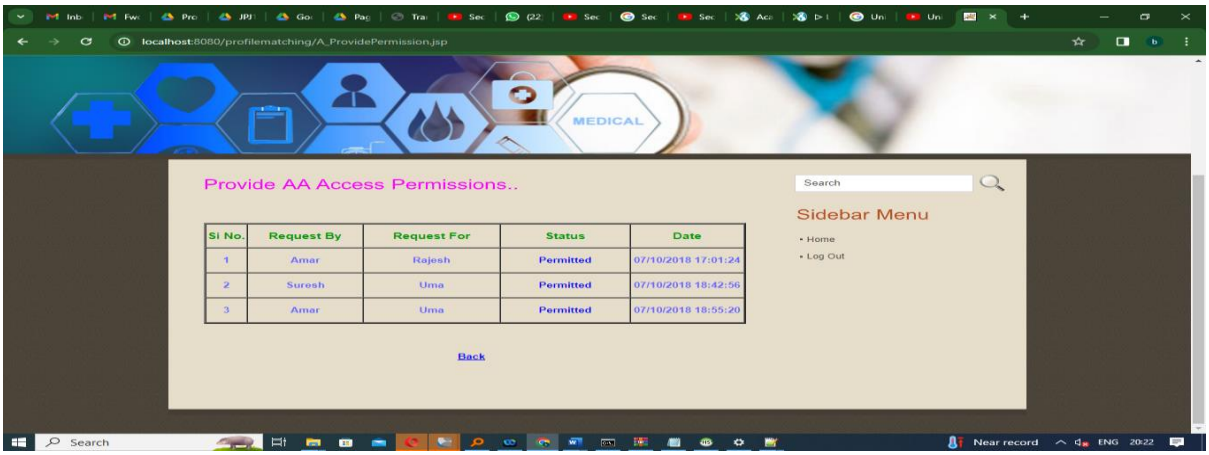


Fig 14:-Providing access permission:

5. CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION:

Because of its easy data exchange, the MHSN has enhanced healthcare. We propose a secure identity-based data sharing and profile matching mechanism in cloud computing with the aim of ensuring data availability and confidentiality in MHSN. We first implement secure data sharing in MHSN using the IBBE cryptographic approach, which enables patients to safely keep electronic health records on cloud servers and effectively share them with a group of physicians. Next, we introduce an attribute-based CPRE method in MHSN that enables physicians to approve the cloud to create a new ciphertext under IBE for the specialist based on a stored ciphertext, without disclosing any private information, provided they meet pre-established requirements. Additionally, we offer an IBEET-based profile matching system that enables flexible authorization on encrypted EHRs.

5.2 FUTURE SCOPE:

It is not feasible to create a system that satisfies every user need. As the system is being used, user requirements are always evolving. Future improvements to this system could include the following: • Upgrading the system and making it flexible to a desired environment when new technologies emerge; • Improving security through the use of emerging technologies like single sign-on in response to developing security challenges.

6. REFERENCES

[1] L. Guo, C. Zhang, J. Sun and Y. Fang, “PAAS: A privacy-preserving attribute-based authentication

system for health networks," in Proc. 32nd International Conference on Distributed Computing Systems, Macau, China, 2012, pp. 224-233.
[2] A. Abbas and S. Khan, "A Review on the state-of-the-art privacy-preserving approaches in the e-Health clouds," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, Jul. 2014.
[3] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in Proc. 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2007, pp. 200-215.
[4] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. 2007 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2007, pp. 321-334.
[5] M. Green, G. Ateniese, "Identity-based proxy re-encryption," in Proc. The 5th International Conference on Applied Cryptography and Network Security, Zhuhai, China, 2007, pp. 288-306.
[6] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans on Parallel and Distrib. Syst., vol. 24, no. 1, pp. 131-143, Jan. 2013.
[7] M. Barua X. Liang, R. Lu and X. Shen, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing," International Journal of Security and Networks, vol. 6, no. 2/3, pp. 67-76, Nov. 2011.
[8] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. 29th Conference on Information Communications, San Diego, CA, USA, 2010, pp. 534-542.
[9] Y. Liu, Y. Zhang, J. Ling and Z. Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing," Future Generate. Compute. Syst., vol. 78, pp. 1020-1026, Jan. 2017.
[10] Y. Yang, X. Liu, R. Deng and Y. Li, "Lightweight sharable and traceable secure mobile health system," IEEE Trans. Depend. Sec Comput., Jul. 2017. [Online]