iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40936

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Survey: Shielded Identity Based Data and Contour Sharing for Mobile Healthcare Through Cloud Computing

Narotam Kumar[1], Prof. Dr Bhuvana J[2]
[1]*Jain University, MCA 3rd Year*
[2]*Jain University*

Abstract: ***Cloud computing is an emerging new technology that can be integrated with healthcare monitoring system. The current survey of all healthcare organizations shows that it needs the assist of cloud computing to store the patients PHI and to get help in emergency condition using cloud-based virtual server. For an effective monitoring system cloud uses BSN to monitor the patient health conditions. Here the cloud acts as a virtual server and stores the patient information in third party server which causes serious threats to security and privacy. The healthcare center contains various approaches which have been used to monitor the healthcare information based on cloud environment. The objective of this study is to discuss about various techniques and taxonomy about the current methods of cloud computing used in hospital healthcare monitoring system. Moreover, the strengths and weaknesses of the healthcare monitoring system approaches are also discussed. The paper will also provide insight into data security policies that may authorize certain administrators to have read-only capabilities for all device parameters and read / write specific set of commands. Each administrator may have a different access profile introduction.***

I. INTRODUCTION

Cloud computing is the latest technology that plays important roles in public and private organization. The main concern of the health care provider is to reduce errors during treatment of patients. Quick access to Cloud allows a member to view patient information and without having to spend time processing its information as in Fig 1. to a third party without the patient's content. Health care systems are primarily divided into two categories of personal and community services and teaching and research activities. Personal health care such as hospital services, patient housing and various departments. Public health care services include medication, diet and safety measures to maintain a friendly environment. Similarly, treatment of infectious diseases is done through educational and research institutions. MOBILE health care is an innovative combination of mobile devices and communication technologies, as it can provide much-needed health information, improvements in general care, potential prevention of infectious diseases, health interventions, etc. It is becoming increasingly cold to use emerging computer technologies. in the portable health sector. Using a portable health care system, an electronic health record (EHR) can be transmitted over the network to a cloud service provider (CSP) for remote storage. In addition, healthcare providers can read it from the end. However, it does not guarantee complete data security and privacy, as many organizations are not qualified enough to add all the layers of security to sensitive data. This paper is a study of data protection strategies used to protect and secure data from clouds around the world. Discusses potential threats to data in the cloud and its solutions adopted by various service providers for data protection. The rest of the paper is arranged as follows. Phase 2 is a review of the literature that provides insight into the work that is already being done in this area. Section 3 discusses the types of threats in the data in the cloud. Section 4 examines some of the data security methods used worldwide. The final section concludes with a summary of this study. Patients have better knowledge of their health care; they are well educated about their illnesses and are increasingly accessing the latest technology that provides greater information about health care. Patients want the best care at the lowest cost and are willing to investigate their own options. As a result, access to patient records is increasing and organizations are required to provide patient record information.

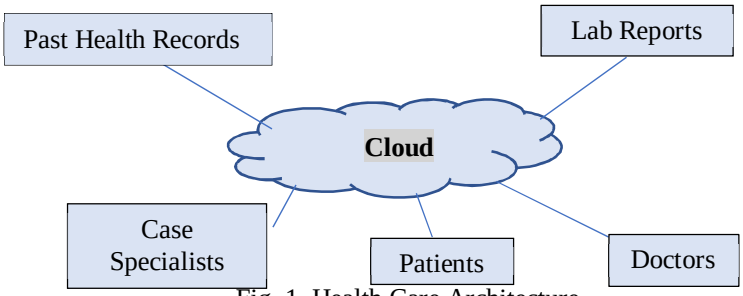


Fig .1. Health Care Architecture

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

It is difficult for patients to understand why they do not have access to their secure global health information such as how a banking system allows customers to withdraw money and access other services anywhere in the world. But health care providers need to be more efficient in terms of cost-effective procedures compared to others, so cloud computing would be a good platform for such a situation. A large number of connected systems, in order to cost and increase the use of automated resources to reduce costs and data usage. In this way hospitals can only provide information if it is needed by a single user without the knowledge of a third party.

II. LITERATURE REVIEW

This Paper introduced Mobile healthcare is an innovative combination of mobile devices and mobile communication technologies, for it can provide necessary health information, routine care improvements, potential infectious disease prevention, health interventions, etc. It is getting more and more widely to apply the emerging cloud computing technology into the fields of mobile healthcare. people tend to share and disseminate the healthcare information via social networks, since social media is an extension of the healthcare professional and patient relationship.

1) Introduction about Ciphertext.

Ciphertext is encrypted text transformed from plaintext using an encryption algorithm. Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key. The decryption cipher is an algorithm that transforms the ciphertext back into plaintext. The term cipher is sometimes used as a synonym for ciphertext. However, it refers to the method of encryption rather than the result.

Example: An unauthorized party to a conversation, even if they intercept our messages, would only possess ciphertext. Without the encryption algorithm and key, they'd never have it in plaintext

2) Cloud Computing Features Especially Like

a) Shared Services: Clients can share resources simultaneously. According to the providers the required resources are distributed but the customer is not fully aware of the areas of demand for services.

b) Extensive Network Access: By using the cloud we can have wider network access using the internet from any devices, anywhere in the world.

c) Extension: Clients can get unlimited usage resources because the cloud is loud and flexible which is free to use. *On-demand self-service:* A customer can configure the cloud automatically without help of service technicians.

A. System Model

Our proposed data-based secure sharing of data and MHSN profile model on cloud computing is shown in Fig. 1, which includes five organizations: central authority, CSP, patient, physician and specialist.

1) The Central Authorities: The central authority is trusted by launching the system and generating attribute keys and private keys for participating users.

2) CSP (Cloud Service Provider): CSP is responsible for archiving data and can be made a proxy as it is less trustworthy. In addition, CSP performs patient profile matching.

3) Patient: The patients register the system to obtain their secret keys with their identities. They encrypt the electronic health record using AES cryptography techniques and the encryption key *K* will be encrypted by an Identity-based broadcast encryption algorithm and outsource the ciphertexts and encryption key to CSP, hence only authorized doctors could decrypt them. Simultaneously, patients with the same symptom can generate trap doors and form social relationships according to their wills.

4) Doctor: Authorized physicians can encrypt patient ciphertext stored in CSP. The authorized doctors can decrypt the patients' ciphertext that stored in the CSP. When encountering a problem that needs to negotiate with a specialist, the doctor can generate a re-encryption request, thus the CSP converts the ciphertext into an IBE-encrypted data for specialist if the doctor satisfies the pre-defined conditions in the ciphertext.

5) Specialist: An expert may remove encrypted ciphertext encryption and help doctors find advice. The specialist could decrypt the re-encrypted ciphertext with the secret key and then assist doctors for advice

©IJRASET: All Rights are Reserved

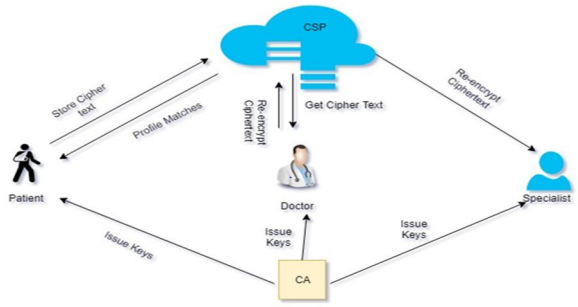


Fig. 1. System model

B. Flexible Authorization

In order to withstand the keywords guessing attack and strengthen the privacy protection, flexible authorization is considered in our scheme. We describe three types of authorization as follows:

1) User to user authorization. Nitin and Ravi generate trapdoors on their all ciphertexts respectively.

2) User to ciphertext authorization. Nitin generates a trapdoor on her all ciphertext, while Ravi generates a trapdoor on his specific ciphertext. Suppose that Ravi suffers from headache and stomachache, but he only wants to find a social friend who has a stomachache. Then he will generate a trapdoor on the stomachache and send it to the CSP.

3) Ciphertext to ciphertext authorization. Nitin and Ravi may have more than one symptom. They generate a trapdoor on one of their ciphertexts according to their inclinations. It also means that they may prefer to find some social friends with part of their symptoms.

III. METHODOLOGY AND EXPERIMENTION

We implement the suggest system with java pairing-based cryptography library to evaluate its performance. The experiments are conducted on a Windows platform.

A. Existing System

However, data security issues are the major obstacles to the application of MHSN. As we all know, health information such as treatment and drug information are considered to be highly sensitive. If these data are outsourced to the CSP, the patients cannot directly control the software or hardware platform for storing data. Without careful consideration, patients may suffer serious medical information leakage from the cloud. For example, millions of EHRs have been compromised in recent years. Hence, it is significant that the EHRs should be stored in an encrypted form. Even if the CSP is untrusted or compromised, the data maintains security and privacy. Simultaneously, the encrypted records should be shared and accessed in a reasonable way.

B. Proposed System

We propose a secure identity-based data sharing scheme for MHSN, which allows patients to outsource their encrypted health records to CSP with IBBE technique, and share them with a group of doctors in a secure and efficient manner. We present an attribute-based conditional data re-encryption construction, which permits doctors who satisfy the pre-defined conditions in the ciphertext to authorize the CSP to re-encrypt the cipher text for specialist, without leaking any sensitive information. We provide an efficient profile matching mechanism in MHSN based on IBE with equality test (IBEET) that helps patients to find friends in a privacy-preserving manner, and achieve flexible authorization on the encrypted health records with resisting the keywords guessing attacks.

C. Privacy Preserving Approaches in eHealth cloud

This paper introduced; Cloud computing is emerging as a new computing paradigm in the healthcare sector besides other business domains. Large numbers of health organizations have started shifting the electronic health information to the cloud environment. Introducing the cloud services in the health sector not only facilitates the exchange of electronic medical records among the hospitals and clinics, but also enables the cloud to act as a medical record storage center. Moreover, shifting to the cloud environment relieves the healthcare organizations of the tedious tasks of infrastructure management and also minimizes development and maintenance costs. Nonetheless, storing the patient health data in the third-party servers also entails serious threats to data privacy

D. Survey on "Proxy re-encryption systems for identity-based encryption"

A proxy re-encryption system allows the proxy to transform ciphertexts encrypted under Ravi's public key into the different ciphertexts that can be decrypted by Nitin'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

E. Survey on "Ciphertext-policy attribute-based encryption"

In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to emp by a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks.

Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

IV. SYSTEM CONFIGURATION

A. Hardware

The Minimum requirement of hardware in the project are as flow:

1) Processor: Minimum 1 GHz; Recommended 2GHz or more
2) Ethernet connection (LAN) OR a wireless adapter (Wi-Fi)
3) Hard Drive: Minimum 32 GB; Recommended 64 GB or more
4) Memory (RAM): Minimum 1 GB; Recommended 4 GB or above

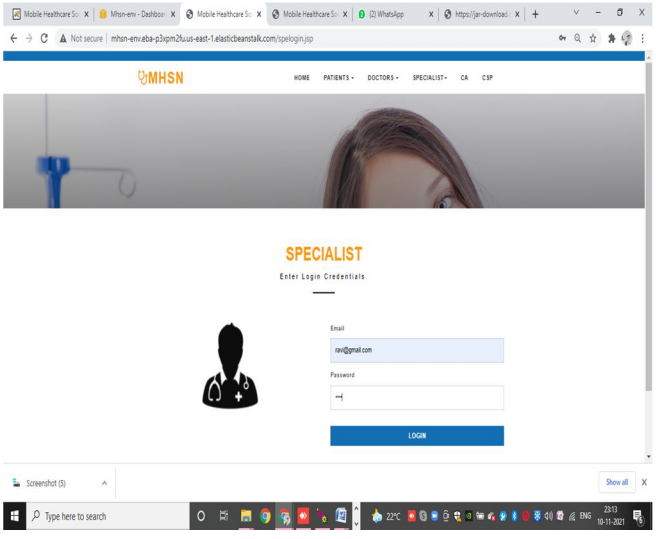
B. Software

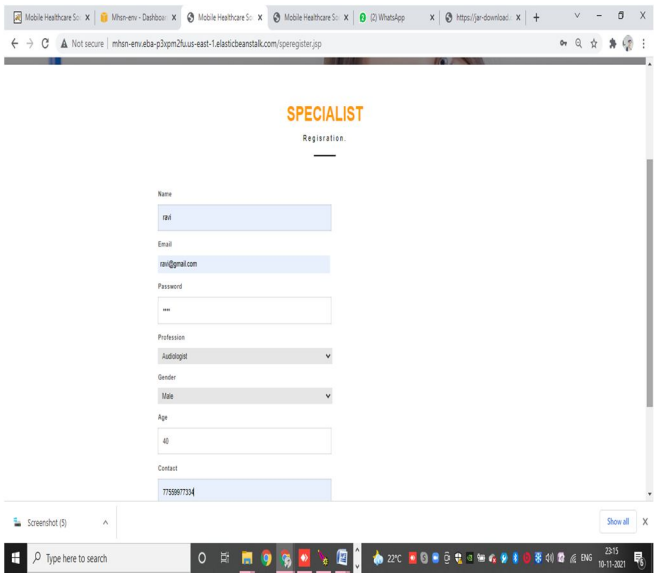
1) Frontend: Html, CSS, Javascript,
2) *Backend:* Elastic Beanstalk

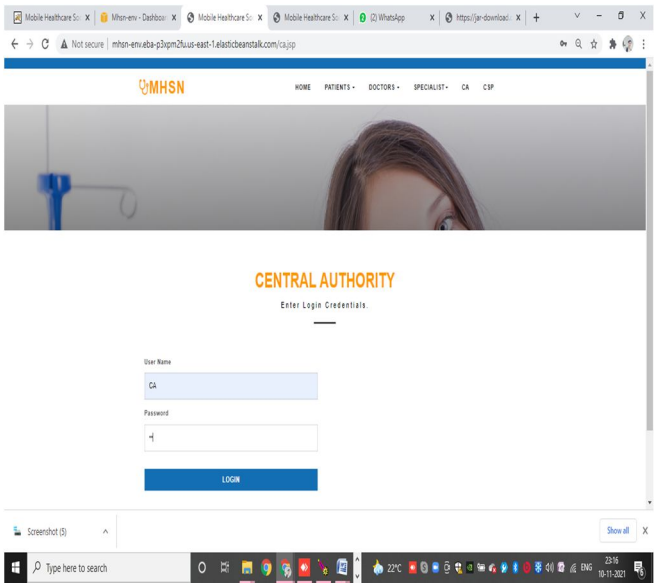
C. Database

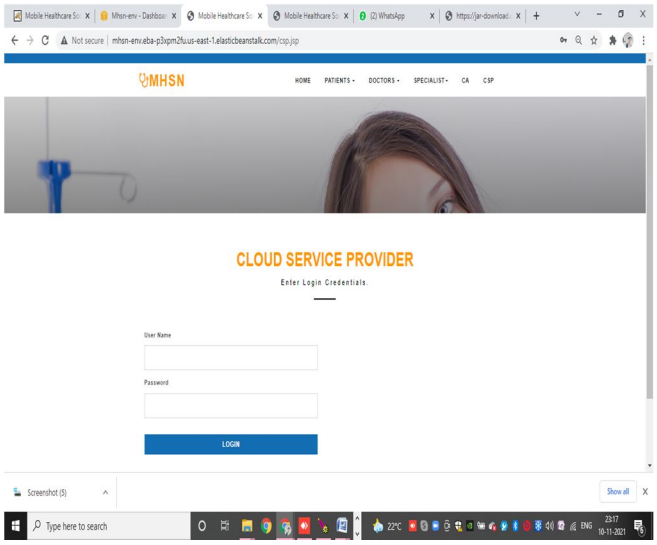
RDS (Relational Databases Service)

The Below listed is the user interface of our proposed application system.




SPECIALIST
Registration.
Name
ravi
Email
ravi@gmail.com
Password
Profession
Audiologist
Gender
Male
Age
40
Contact


MHSN
HOME
PATIENTS
DOCTORS
SPECIALIST
CA
CSP
CENTRAL AUTHORITY
Enter Login Credentials.
User Name
CA
Password
LOGIN

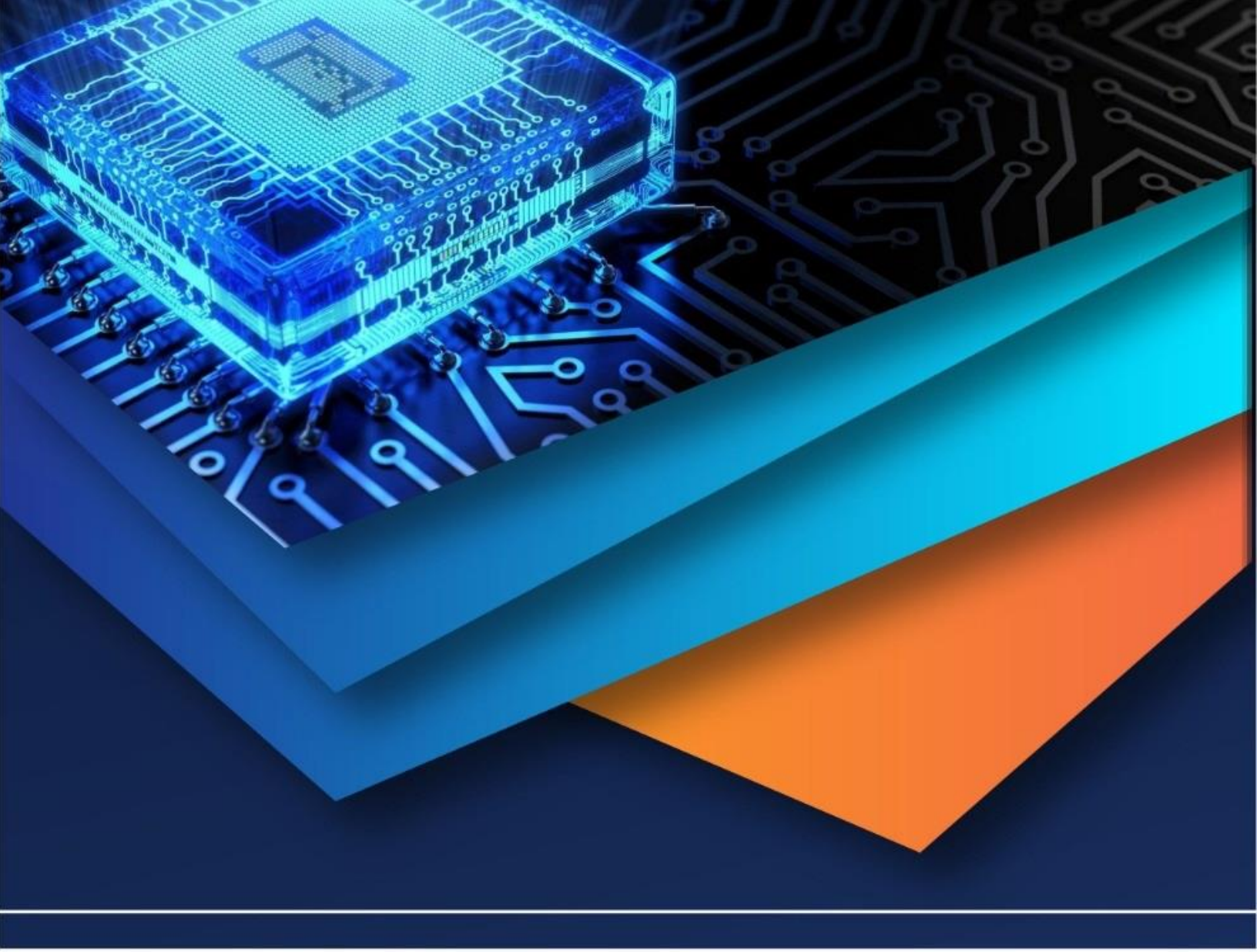

MHSN
HOME
PATIENTS
DOCTORS
SPECIALIST
CA
CSP
CLOUD SERVICE PROVIDER
Enter Login Credentials.
User Name
Password
LOGIN

V. CONCLUSION

The MHSN has changed the healthcare by its suitable data sharing. For the purpose of guaranteeing data confidentiality and availability in MHSN, we suggest a secure identity-based data sharing and profile matching scheme in cloud computing. We notice secure data distributing in MHSN with IBBE cryptographic technique, which allows the patients to store HER so cloud securely and split them with a group of doctors precisely. Then we present an attribute-based CPRE mechanism in MHSN, which allows doctors who please the pre-defined state to allow the cloud to transform a stored ciphertext into a new ciphertext under IBE for the specialist, without breaching any sensitive data. we provide a profile matching procedure based on IBEET, which can attain flexible authorization on encrypted EHRs and helps the patients to find friends in a privacy preserving &efficient way. The analysis and results show that the computation cost on patient side is reduced.

REFERENCES

[1] 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.
[2] 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.
[3] 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. 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
[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC00, 2000, paper 11.3.4, p. 109
[5] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61
[6] Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing,Qinlong Huang, Member, IEEE, Wei Yue, Yue He, Yixian Yang, Jul. 2018
[7] 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.
[8] 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
[9] M. Li, N. Cao, S. Yu and W. Lou, “FindU: Privacy-preserving personal profile matching in mobile social networks,” in Proc. 2011 IEEE International Conference on Computer Communications, Shanghai, China, 2011, pp. 2435-2443.
[10] R. Zhang, J. Zhang, Y Zhang, J. Sun and G. Yan, “Privacy-preserving profile matching for proximity-based mobile social networking,” IEEE J. Sel. Areas Comm., vol. 31, no. 9, pp. 656-668, Sept. 2013.
[11] L. Wu, Y. Zhang, K. Choo and D. He, “Efficient and secure identity-based encryption scheme with equal



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)