

PRIVACY PROTECTION AND INTRUSION AVOIDANCE FOR CLOUDLET-BASED MEDICAL DATA SHARING

V.Sarala¹, Bunga Praveen²,

¹Assistant professor , PG DEPT, Dantuluri Narayana Raju College, **Bhimavaram, Andharapradesh**

Email:- vedalasarala21@gmail.com

²PG Student of MCA, Dantuluri Narayana Raju College, **Bhimavaram, Andharapradesh**

Email:- bungapraveen7702@gmail.com

ABSTRACT

With the popularity of wearable devices, along with the development of clouds and cloudlet technology, there has been increasing need to provide better medical care. The processing chain of medical data mainly includes data collection, data storage and data sharing, etc. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves users' sensitive information and causes communication energy consumption. Practically, medical data sharing is a critical and challenging issue. Thus in this paper, we build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the stage of data collection, we first utilize Number Theory Research Unit (NTRU) method to encrypt user's body data collected by wearable devices. a new trust model to help users to select trustable partners who want to share stored Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, we present data in the cloudlet. The trust model also helps similar patients to communicate with each other about their diseases. Thirdly, we divide users' medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks. . Our experiments demonstrate the effectiveness of the proposed scheme.

1 INTRODUCTION

Currently electronic medical records (EMRs are very prominent in healthcare networks. They enables users to share their data in a flexible and convenient way. For example, to find one's diagnostic report, a patient or his/her doctor needs only to retrieve the information from a database rather than having to search Through numerous physical documents. Health data is very sensitive, and it is a major challenge to securely store and access EMRs in modern EMR systems. As most EMRs are outsourced to the cloud, they are easily exposed to potential threats and vulnerable to breakage loss and theft [1]To prevent EMRs from unauthorized access a standard solution is to perform an encryption before uploading them to the cloud. Specifically an EMR owner encrypts an EMR using a symmetric key, and only authorized medical staff are authorized to access and decrypt it. However, data sharing becomes the complicated key management and repetitive encryption [2]:as patients us all do not know who is allowed to access their EMRs, they encrypt many pieces with distinct session

keys and distribute the keys to different medical staff members. The approach to accessing users' data needs to be flexible enough to address changes in users' roles [3].

Literature Survey

K.Hung, Y.Zhang ,and B.Tai,“ We are able tele home health care emergency supplies," This paper describes a method that attempts to constantly monitor a patient from indoor or outdoor settings. The device is focus on a patient carried Bluetooth PAN ,whose central node ,a mobile phone, compiles details about the position and health condition of the patient. Such information is secured in order to be transmitted via Wifi or GPRS/UMTS to a server. The frame work offers facilities for obtaining patient records, including from a J2ME programme from a mobile phone .It also helps the threshold values used to define emergency conditions to be remotely configured. M.S. Hossa in," The cyber physical localization frame work for patient monitoring supported by the cloud," The promise of cyber-physical systems (CCPSs) enabled by the cloud has attracted a great deal of attention from academia and industry. CCPSs encourage the smooth in corporation with cyber space with technologies in the real environment (e.g. sensors, cameras, microphones, speakers, and GPS devices). This allows for a variety of new Technologies or frameworks that enable patient positions to be monitored, such as patient or wellness tracking.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

- ❖ Access control [11] is widely adopted in the EMR system to protect patients' health data. Access control policies are specified by some pieces of legislation, i.e., health insurance portability and accountability act (HIPAA) [12], electronic documents [13], and company rules or regulations. The legislation regulates who can access and how they can operate the stored EMRs. Two solutions are usually used to support flexible access control. One solution is to use attribute based encryption [14], [15]. As attributes can be applied to describe users' privileges, data owners determine the access policies. The other solution is to use role-based access control schemes [8], where each user's identity denotes a role and one is allowed to gain access permission if his role belongs to a defined policy.

Disadvantages:

- The system is not implemented to provide secure electronic medical record.
- The system is not implemented Privacy Preservation for Outsourced Medical Data.

Proposed System & algorithm

In the proposed system, the system designs two anonymous schemes, denoted as “*RBA-CAnonym*” and “*RBACAnonym-F*”, to preserve patients' privacy in an EMR system with role-based

access control. We present competing models and a high level demonstration of rigorous proof. In brief, our schemes have the advantage of data confidentiality, identity anonymity and access control flexibility. Technical details are highlighted as follows. *RBACAnony*. This scheme is built on a bilinear group with two subgroups [9], and a patient's identity information is hidden in one of the subgroups.

4.1 Advantages:

- **Data Confidentiality.** Personal data needs to be encrypted before being uploaded and securely stored on the cloud until an entitled recipient downloads and decrypts it. Specifically, only the users whose roles satisfy the associated access policy have the privilege to access the data, with all other unauthorized entities not able to obtain any useful information from the encrypted data, even if they collude with each other.
- **Identity Anonymity.** Identity-related information needs to be hidden, as individual privacy is vulnerable to loss, theft, and illegal transactions. When a user's identity is hidden in an EMR system, it decreases the possibility of an adversary guessing that user's identity such that hardly any third party can obtain useful patient information.

IMPLEMENTATION

MODULES

- **Service Provider**

In this module, the data owner performs operations such as Upload Patient Details, Update Patient Details, View End User Transactions, View End User Search History

USER

In this module, he logs in by using his/her user name and password. After Login receiver will perform operations like View My Profile, Request Permission, Request Response Details, Searches files based on Patient, My Search History, My Transaction

Trusted Authority

In this module, the sector can do following operations such as Give Privileges to Users, View All Blocked Attackers

5 RESULTS AND DISCUSSION

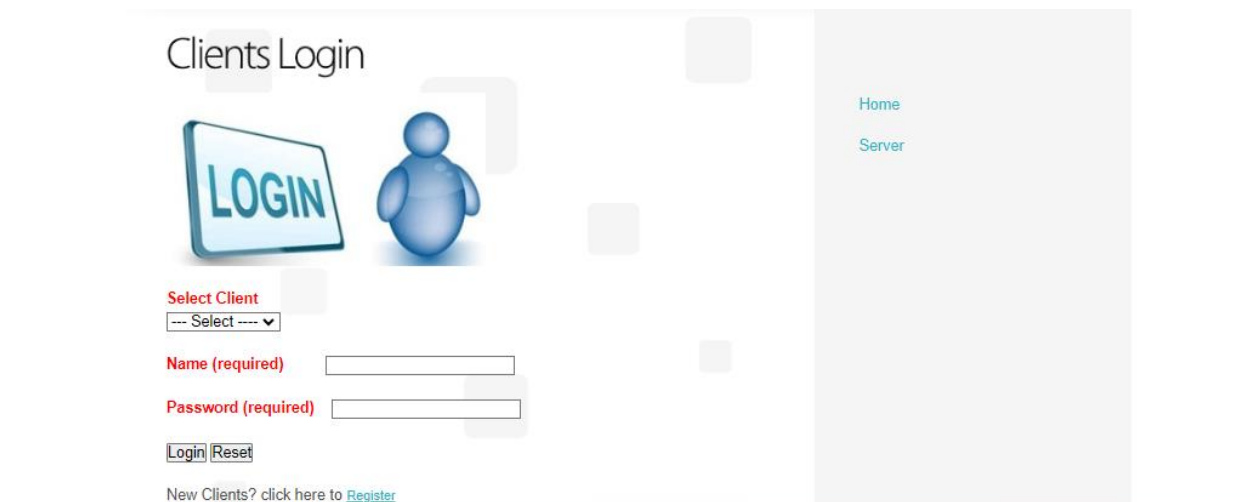
SCREENSHOTS

HOME PAGE



Figure HOME PAGE

CLIENTS LOGIN



The screenshot shows the 'Clients Login' interface. At the top left, the title 'Clients Login' is displayed. Below it is a graphic featuring a blue monitor with the word 'LOGIN' and a blue 3D human figure. The login form includes a 'Select Client' dropdown menu with a placeholder '--- Select ---'. Below this are two text input fields labeled 'Name (required)' and 'Password (required)'. At the bottom of the form are two buttons: 'Login' and 'Reset'. A link 'New Clients? click here to Register' is located at the bottom left. On the right side, there is a vertical sidebar with two links: 'Home' and 'Server'.

Clients Login

Home
Server

LOGIN

Select Client
--- Select ---

Name (required)

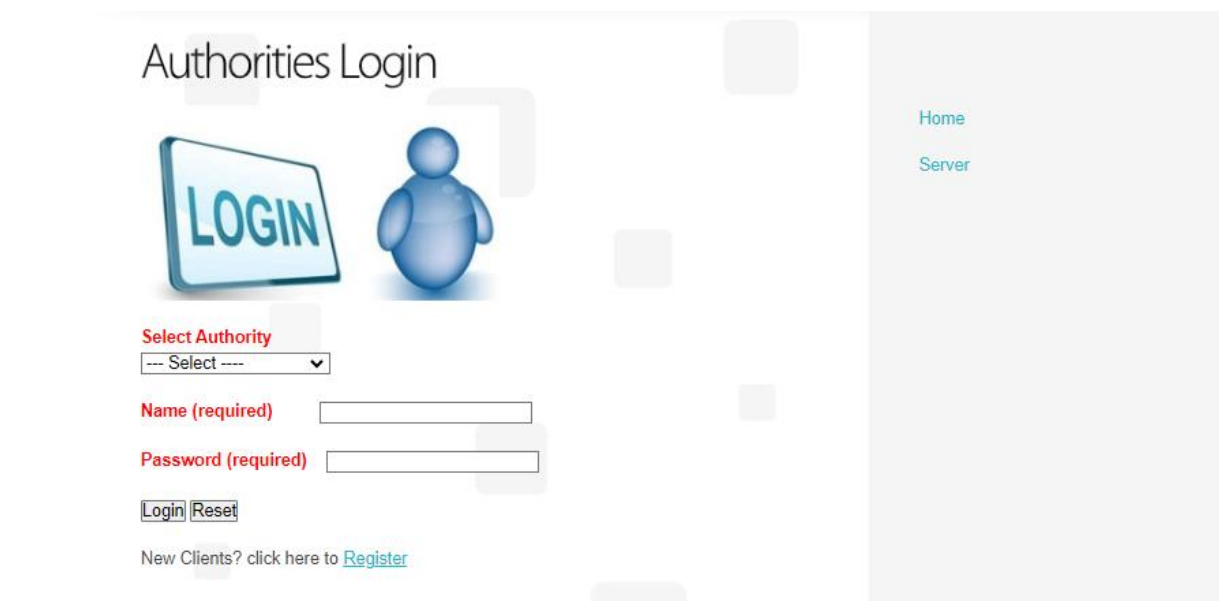
Password (required)

Login Reset

New Clients? click here to [Register](#)

Figure CLIENTS LOGIN

AUTHORITIES LOGIN



The screenshot shows the 'Authorities Login' interface. At the top left, the title 'Authorities Login' is displayed. Below it is a graphic featuring a blue monitor with the word 'LOGIN' and a blue 3D human figure. The login form includes a 'Select Authority' dropdown menu with a placeholder '--- Select ---'. Below this are two text input fields labeled 'Name (required)' and 'Password (required)'. At the bottom of the form are two buttons: 'Login' and 'Reset'. A link 'New Clients? click here to Register' is located at the bottom left. On the right side, there is a vertical sidebar with two links: 'Home' and 'Server'.

Authorities Login

Home
Server

LOGIN

Select Authority
--- Select ---

Name (required)

Password (required)

Login Reset

New Clients? click here to [Register](#)

Figure AUTHORITIES LOGIN

SERVER LOGIN

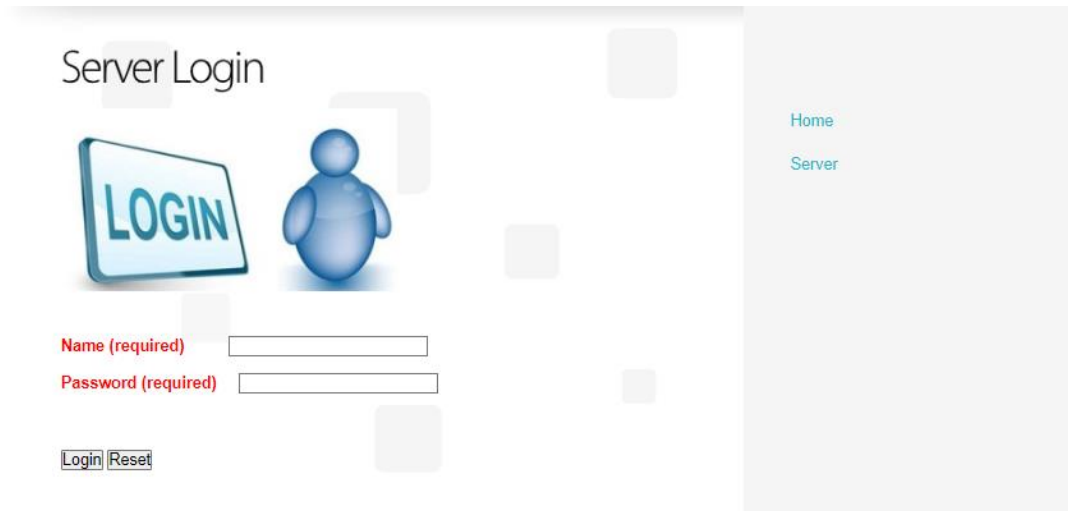


Figure SERVER LOGIN

6. CONCLUSION AND FUTURE WORK

CONCLUSION

In this paper, we propose two anonymous RBAC schemes for the EMR system. We achieve flexible access control such that the EMR data can be encapsulated according to an on demand access policy, with only users whose roles satisfy the access policy being able to decapsulate it. Patients' privacy is preserved using a bilinear group, where all the identity related information is hidden in a sub group. Based on the chosen bilinear group assumptions, we prove that our proposed model has the property of semantic security and anonymity. We apply the "online/ offline" approach to achieve a better user experience.

7. REFERENCES

- [1] M. J. Atallah, M. Blanton, and K. B. Frikken, "Dynamic and efficient key management for access hierarchies," *ACM Trans. Inf. Syst. Secur.*, vol. 12, no. 3, pp. 190–202, 2009.
- [2] J. Huang, M. Sharaf, and C. T. Huang, "A hierarchical framework for secure and scalable EHR sharing and access control in multi-cloud," in *Proc. ICPPW IEEE*, Sep. 2012, pp. 279–287.
- [3] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care," in *Proc. 14th Int. Workshop Database Expert Syst. Appl.*, Sep. 2003, pp. 432–437.
- [4] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. J. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in *Proc.*

SPSMACM , 2011, pp. 75–86.

[5] S. Narayan, M. Gagné, and R. Safavi-Naini, “Privacy preserving EHR system using attribute-based infrastructure,” in Proc. CCSW ACM, 2010, pp. 47–52

. [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. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[7] M. Sicuranza, A. Esposito, and M. Ciampi, “A view-based access control model for EHR systems,” in Intelligent Distributed Computing—IDC. Cham, Switzerland: Springer, 2014, pp. 443–452.

[8] W.Liu, X.Liu, J.Liu, Q.Wu, J.Zhan, and Y.Li, “Auditing an revocation enabled role-based access control over outsourced private EHRs,” in Proc. HPCC IEEE, Aug. 2015, pp. 336–341.

[9] D. Boneh, E.-J. Goh, and K. Nissim, “Evaluating 2-DNF formulas on ciphertexts,” in Theory of Cryptography—TCC. Berlin, Germany: Springer, 2005, pp. 325–341.

[10] A. De Caro, V. Iovino, and G. Persiano, “Fully secure anonymous HIBE and secret-key anonymous IBE with short ciphertexts,” in Proc. Int. Conf. Pairing-Based Cryptogr., 2010, pp.
