INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING

ISSN: 2320-1363

Enhance Secure Data sharing Using Petri Nets based Certification in Cloud Computing

K.Ashoka Rani*1, K.Janardhan*2

M.Tech (CSE) Student, Dept of CSE, Intell Engineering College, D.t: Anantapur, A.P, India

Assoc.Prof, Dept of CSE, Intell Engineering College, D.t: Anantapur, A.P, India

ABSTRACT

Business applications are prefer cloud computing services. Cloud computing establishes with good internet services. In cloud service providers store the patient health records (PHRs). Exchanges patient health records as a secure outsource data. Existing system work some security constraints are missing. In data transmission time some issues or risks are generate with previous privacy approaches [4][5]. Those approaches are key management, attribute encryption techniques and third party auditors. These approaches are not accurate, efficient and scalable. These approaches are not control and prevent issues in access data and exchanges the data [6][7].

In proposed work some new security constraints we add to increase the security and accuracy levels in data sharing. These new approaches are enhances the security in data sharing. Those approaches are Petri nets, certification and homomorphic encryption schemes. Certification approach introduces challenge response protocol. This present protocol verifies in each and every level. In transmission time control all privacy and show the performance with increased scalability and efficiency [5][6].

KEYWORDS: **Challenge Response Protocol, Petri Nets. Key Management operations.**

I.INTRODUCTION

Cloud Computing is present growing and tremendous technology. Cloud computing contains the data storage with remote servers. All applications are uses the data storage as a remote servers. Present applications some issues are related loss privacy details. Private data it may chance to loss in data sharing time in different applications maintenance [2][4][6].

Privacy data loss problems are generate people are face the problems. In holidays time sometimes gets the problem related to unavailability issues. These problems we observe in present cloud servers applications. We observe many issues related in many number of health service providers. Those problems like leakage data. Outsider attackers are creates some issues related like leakage and data loss. Its shows the performance related issues like low scalability and low efficiency.

Increases the scalability and efficiency performance levels are major goals in proposed system in data sharing with cloud service providers. Excellent way to control the issues using Petri nets, certification based approach, homomorphic encryption process and last we use the cryptography related approaches also.

II.BACKGROUND STUDY

E-Health Systems are completely related to store the data and process the data in cloud. Process task is related to outsource the data. In outsourcing time we need one good security platform or framework. New security platform control different security issues and decreases the cost and complexities in implementation. Using these new techniques we improve the security in transmission of electronic Health records [1] [2] [3].

Basic fundamental problem we consider here in accessing of records previous techniques are not support to deliver authentication records. Related Previous techniques some demerits are available. We discuss about previous techniques in following paragraphs.

One of the encryption methods is introduced authentication for EHRs in transmission or exchange. All PHR or EHR are encrypting using some encryption techniques. Records are converts into cipher text format. In destination users are access using decryption keys. We display original data. Normal encryption techniques have less number of keys. This type of key management technique is not gives the scalability and efficiency solution [4].

ISSN: 2320-1363

Another method, control the Electronic Health Record we use policies. Policies are creating with rules. These policies are gives the trust related solutions. Policies are implementing in health service providers areas.

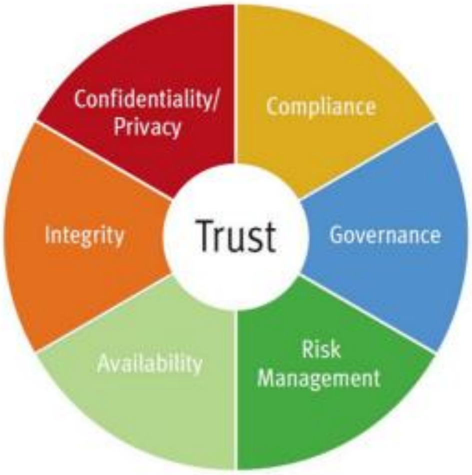


Fig. 2.1 **Trusted Policy creations with different policies.**

Policies creations are two types. One is role based policy; another one is related to attribute related policy. These are provided the security or privacy in physical locations. We expect the security in cloud environment. It's hard to provide the privacy in cloud servers data maintenance specification [1][5][6]. The above two policies are not trusted in implementation.

After some number of days in cloud service infrastructure some changes are generate to increase the privacy or security. In cloud data storage for auditing purpose we add TPA (Third Party Auditor). Owner uploads the PHRs into cloud server. Users are forward the request to CSP. Users are starting the download of records. TPA start the verification users are authorized or not. After using TPA we are not gives guarantee to provide authentication results. Present cloud computing infrastructure also show the problems related to security and privacy [6] [7].

Another method, patient centric model works using multiple data owners and trust worth attribute related policies. After implementation of above approaches its not gives the sufficient privacy.

The above all techniques are not gives the 100% guarantee to provide the privacy. All are centric models working procedures [1][2][3][4][5][6][7].

III.PROBLEM STATEMENT

We introduce New Rule patterns like Petri Nets in verification to access the personal health records or Electronic Health records. These rule patterns we use into work flow of application. In workflow compilation implement some business languages. Those languages are BPMN (Business Process Modeling Notations), BPEL (Business Process Execution Language), and Event Driven Process Chain (EPC). HIPAA organization introduces some new rules with good policies. Local health and global health service providers are contains different policies. Using those policies verifies the PHRs or EHRs and filter protected health records by authorized users. All users are satisfies the linear rules with good correlation. In each and every rule place the flag related solution with decision making. Each rule nothing but attribute. Any user can access the records cloud service provider verifies the all attributes linearly. All attributes are correct, those users are certification users. Those users are access the personal health records information. This complete working procedure related like homomorphic encryption technique. Its gives guaranteed privacy results to access the result without leakage [7] [8].

IV.SYSTEM MODEL

New system we proposed for secure data sharing using Petri nets. All Patients records stored in cloud server. Any patient can access the data we control the data of cloud server. Using Petri nets without keys maintenance control the data. These all Petri nets are used in workflow to access the data. For providing good security we added the verification providers like local and global. All types of providers verify based on attributes and control the attackers in implementation process [10][11].

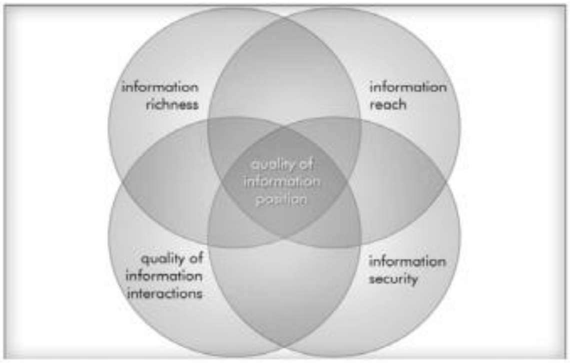

information richness
information reach
quality of information position
quality of information interactions
information security

Fig3.1.1: **Steps exchanges secure data sharing**

Cloud servers to user's access data transmission we expect good outsource data delivery. Transmission stage we follow some rules then only deliver data as a quality. Cloud server starts the transmission with good security constraints as a attributes. Authorized user interacts with all attributes, all attributes are verified as an authenticated, and then to exchanges the personal health record effectively. This is good information exchanges richness (Fig1).

Petri Nets are used workflow compilation process with good rule adherence. These rules are providing the good influence to control the attackers. Using those attackers its possible exchanges secure data sharing [9].

In Petri nets add the some encryption techniques to control the data. All Personal health records information maintains as a cipher text format. Using the attribute based rules encrypted without leakage exchanges effectively. All leakage problems are controlled with the help of homomorphic encryption techniques. It's very good techniques in verification of records.

In Homomorphic verification technique we use the protocol is challenge response protocol. Any user can access the data, through each and every request forward the challenge. It's verified by the cloud service provider with third party auditor. Challenge is verified those patients are access the personal health records. PHR delivered successfully without modified that verification also possible by challenge response protocol [11][12].

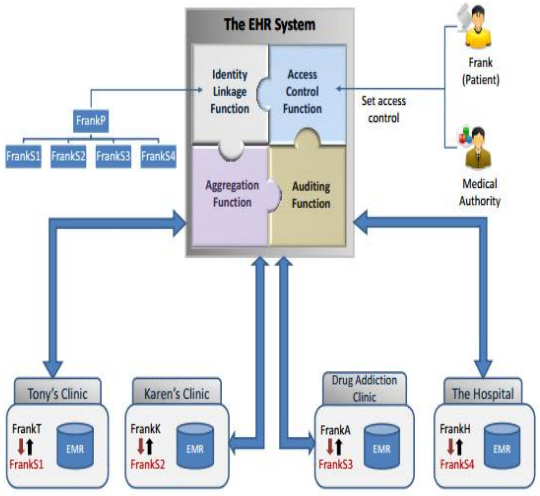
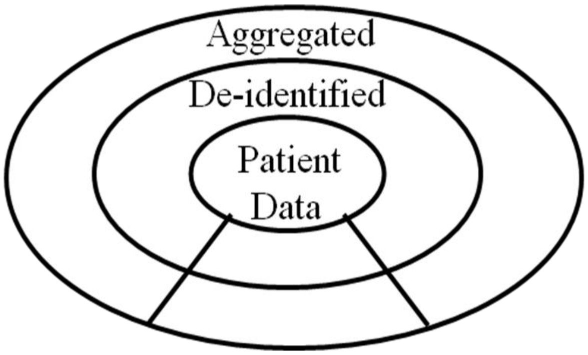


Fig 3.1.2 **Verification using Aggregation and Auditing Functions**

Fig 3.1.2 Exchange the data from one clinic data storage to user we place verification functions. Those verification functions are decides to access the data. All users are satisfies the identity management in auditing environment, those users are access the data.

V. Proposed System Architecture



Patient data access by only identified users. This complete procedure related to layer design. In each and every we tune for detecting the misbehavior users. All layers of rules at last identified in destination point, then only we allow accessing the PHR, in download or access the PHR we apply the homomorphic encryption technique in implementation.

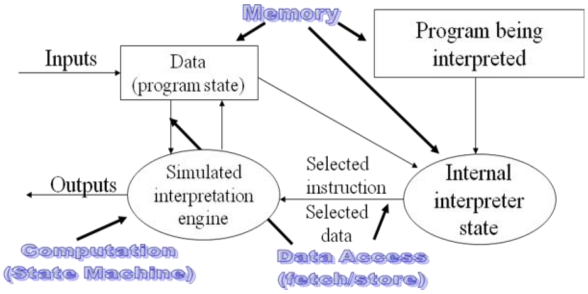
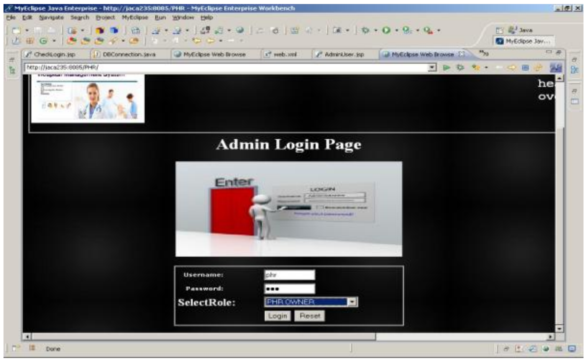


Fig 4.1 **Workflow with state diagram**

Every level consider as a state. In state three steps are available. One is input stage: select PHR. In PHR apply the instructions in data sharing. All instructions are working properly then to allow the data. All authentication users are access the encrypted data. Complete encrypted data is possible to decryption successfully.

V.EXPERIMENTAL EVOLUTION

One of new prototype we implement for enhance the data security. Normal user enters user name, password and select the role.



MyEclipse Java Enterprise - http://jaca235:8085/PHR - MyEclipse Enterprise Workbench

http://jaca235:8085/PHR/

Admin Login Page

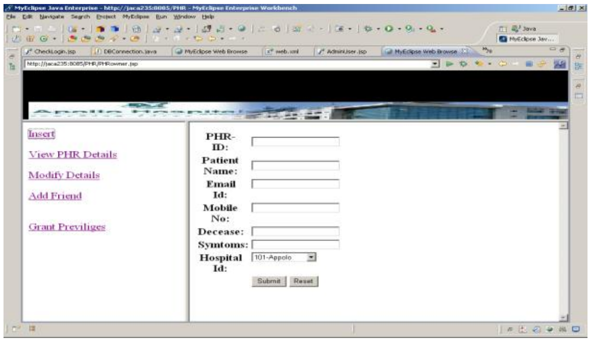
Username: phr

Password: ●●●

SelectRole: PHR OWNER

Fig 5.1 Login Form

Insert the new PHR in data base and automatically update in database.



MyEclipse Java Enterprise - http://jaca235:8085/PHR - MyEclipse Enterprise Workbench

http://jaca235:8085/PHR/PHRowner.jsp

PHR-ID:

Patient Name:

Email Id:

Mobile No:

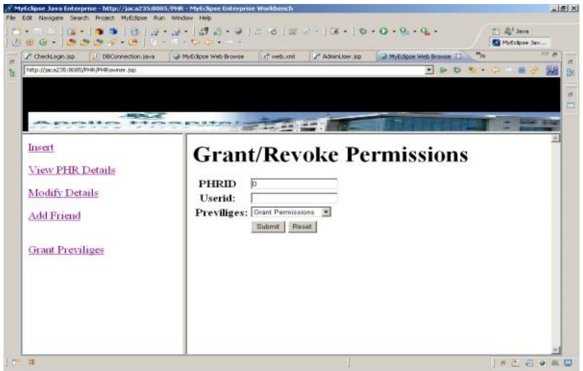
Decease:

Symtoms:

Hospital Id: 101-Appolo

Fig5.2 Insert new PHR

PHR owners provides the permissions to each and every normal users. Those permission related screenshots is available below



MyEclipse Java Enterprise - http://jaca235:8085/PHR - MyEclipse Enterprise Workbench

http://jaca235:8085/PHR/PHRowner.jsp

Grant/Revoke Permissions

PHRID 0

Userid:

Previliges: Grant Permissions

Fig 5.3 Grant or Revoke Permissions

This complete application show the difference with different privacy approaches. Those approaches are normal attribute encryption techniques to Petri Nets with certification. Our petri nets show the good performance compare to all approaches.

VI. CONCLUSION AND FUTURE WORK

In previous modern applications some existing techniques are used. These techniques are not provide the good accuracy and efficiency and scalability in secure data sharing. In proposed work we added the new approach like petri nets. This new approach gives the good solution in security and privacy issues. Its gives the good accurate results compare to previous all approaches. In Future work its may chance reduces overhead and scalability of work procedure. Security and privacy approach is completely future approaches and increases to provide the good quality.

VII.REFERENCES

1. A Homomorphism Encryption Technique for Scalable and Secure Sharing of Personal Health Record in Cloud Computing, Soubhagya B, Venifa Mini G, Jeya A. Celin J, 2013.
2. State of The Art and Hot Aspects in Cloud Data Storage Security, Nicolae Paladi, Christian Gehrmann, Fredric Morenius, 2013.
3. Business Transformation through Cloud Computing, Neil McEvoy, 2013.
4. Shared and Searchable Encrypted Data for Untrusted Servers, Changyu Dong1, Giovanni Russello2, Naranker Dulay1, 2009
5. Secure Management of Personal Health Records by Applying Attribute-Based Encryption, Luan Ibraimi#*1, Muhammad Asim#2, Milan Petkovic#3, 2012
6. Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings, Ming Li1, Shucheng Yu1, Kui Ren2, and Wenjing Lou1, 2010
7. DACC: Distributed Access Control in Clouds, Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic, 2011.
8. Fuzzy Petri Nets, 2011
9. Structural and Dynamic Changes in Concurrent Systems: Reconfigurable Petri Nets, 2004, Marisa Llorens and Javier Oliver.
10. Adaptive fuzzy petri nets for dynamic knowledge representation and inference,2000
11. Modeling Security Architectures for the Enterprise, 2009
12. PetriNets: Properties, Analysis and Applications, 1989.