International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Patient Privacy Control for Health Care in Cloud Computing System

Farheen Pathan[1], Prof. Jadhav H. B.[2]

[1]*PG Student, Vishwabharati Academy's College of Engineering, Ahmednagar.*
[2] Professor, Dept. of Computer Engineering, *Vishwabharati Academy's College of Engineering, Ahmednagar.*

Abstract - *Distributed Healthcare cloud computing system provides proper treatment to the patient for medical consultation by sharing personal health information among healthcare providers. It is having the challenge of keeping both the data confidentiality and patient's identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be exploited straightforwardly.*

This system is designed and developed under simulative approach for patient doctor application development for interconnecting the patient with doctor. The application is more reliable and scaled under performance .The system is under cloud computing simulative approach. The project focuses on the application development under ongoing and hyperactive mode of connectivity for data exchange modeling. This system is similar to that of remote infrastructure development . The overall system design is an approach for telemedicine approach.

***Key Words*: Authentication, access control, distributed cloud computing, healthcare system, security and privacy.**

1.INTRODUCTION

Cloud computing is a delivery of on demand computing resources. Everything from application to data centers over the internet on a pay for use basis. Distributed cloud computing is the application of cloud computing technologies ti interconnect data and application server from multiple geographic locations. Healthcare organization turn to cloud computing to save on the cost of storing hardware locally The cloud holds big datasets for EHRs, radiology, images. Cloud computing offers significant benefits to the healthcare sectors, doctors clinic ,hospitals require quick access to computing and large storage facilities which are not provided in the traditional settings. But before this it takes more time. Cloud caters provides the opportunity to improve services to their customers, patients to share information more easily than even before and improve operational efficiency at the same time.

The system designed and developed in this way that it will be more secure and reliable under action of fetching plan is stable and most beneficial information under patient doctor interaction. This is improved and analyzed under this system. Basically the system is simulated for achieving the terminology of telediagnosis and telemedicine. In general the system is more reliable and trusted under basic contribution of diagnosis. In this project the system administrator, doctors and patient are actors and with an add-on feature of lab staff. This close analysis and behavioral approach is mode a remarkable step in analyzing and understanding the system.

2. Literature Survey

In paper Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment, F.W. Dillema and S. Lupetti(2007), proposed a scheme protect against aggregation threats without letting the patients carry their own medical data. The drawback of this system is that patient and health worker need to meet in the physical world.

In paper FDAC: Towards Fine-grained Distributed Data Access Control in Wireless Sensor Networks ,S. Yu, K. Ren and W. Lou (2009) proposed scheme that exploits a novel cryptographic primitive called attribute based encryption (ABE), tailors, and adapts it for WSNs with respect to both performance and security requirements.The drawback of this system is low fine grained access control

In paper SAGE: A Strong Privacy preserving Scheme against Global Eavesdropping for E- health Systems, X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato (2009) proposed a strong privacy preserving Scheme Against Global Eavesdropping, named SAGE, for e-Health systems. The proposed SAGE can achieve not only the content oriented privacy but also the contextual privacy against a strong global adversary. The drawback of system is they mainly study the issue of data confidentiality in the central cloud computing architecture.

In paper Privacy and Emergency Response in Ehealthcare Leveraging Wireless Body SensorNetwork, J. Sun, Y. Fang and X. Zhu (2010) This scheme provide detailed discussions on the privacy and security issues in e-healthcare systems and viable techniques for these issues.

In paper Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings, M. Li, S. Yu, K. Ren and W. Lou (2010) proposed a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained and scalable access control for PHRs, to leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR data.

3.Architecture

The system architecture consists of patient unit, doctor unit, lab unit as the external compotator for accessing and retrieving information as the system modeling behavior. The overall system is designed and developed under a closed pattern of system environment. Typically the system is authenticated and enhanced under the system modeling nature of performance estimation.

Under this approach, the system is imitated with a data centric memory modeling array for conducting and correlating the patient application. The patient on registration is requested to fill the application form and thus retrieve the system approach and behavior for simultaneously developed model.

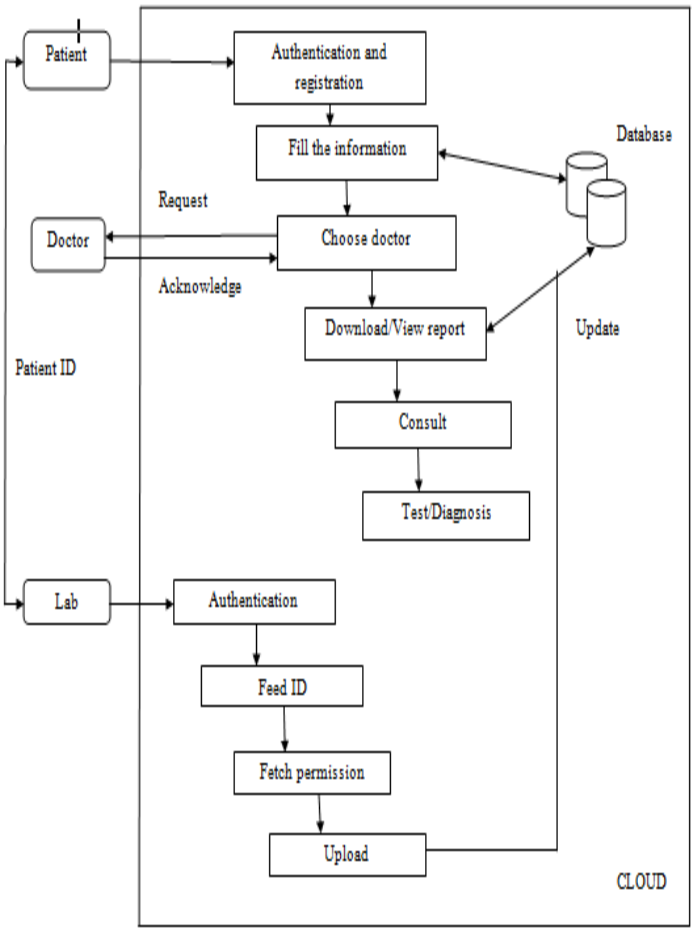

Fig -1: Architecture of System

4.Algorithm

A system is developed for patient self-controllable and multilevel privacy-preserving and cooperative authentication scheme (PSMPA) based on ADVS to realize three levels of security and privacy requirement in distributed m-healthcare cloud computing system which mainly consists of the following five algorithms:

- Setup
- Key Extraction
- Sign
- Verify
- Transcript simulation Generation
- Correctness

Denote the universe of attributes as U. We say an attribute set ω satisfies a specific access structure A if and only if A(ω) = 1 where ω is chosen from U. The algorithms are defined as follows. Setup. On input 1l, where l is the security parameter

• **Setup:** On input 1l, where l is the security parameter, this algorithm outputs public parameters and y as the master key for the central attribute authority.

• **Key Extract:** Suppose that a physician requests an attribute set ωD ∈ U. The attribute authority computes skD for him if he is eligible to be issued with skD for these attributes.

• **Sign:** A deterministic calculation that uses the patient's private key skP , the uniform open key pkD of the human services supplier where the doctors work and a message m to produce a mark σ. That is, σ ← Sign(skP , pkD,m).

• **Verify:** Assume a physician wants to verify a signature σ with an access structure A and possesses a subset of attributes ωJ ⊆ ωD satisfying A(ωJ) = 1, a deterministic verification algorithm can be operated. Upon obtaining a signature σ, he takes as input his attribute private key skD and the patient's public key pkP , then returns the message m and True if the signature is correct, or ⊥ otherwise. That is, {True, ⊥} ← V erify(skD, pkP , m, σ).

• **Transcript Simulation Generation:** It requirse that the directly authorized physicians who hold the authorized private key skD can always produce identically distributed transcripts indistinguishable from the original protocol via the Transcript Simulation algorithm. Due to the fact that the Transcript Simulation algorithm can generate identically distributed transcripts indistinguishable from the original signature σ, the patient's identity can be well protected from the indirectly authorized physicians for whom only the transcripts are delivered. In addition to the main algorithms described above, we also require the following properties.

• **Correctness.** All signatures generated correctly by Sign would pass verify operated by the directly authorized physicians.

5. Pseudo code

Step 1: Environment setup and alignment

Step 2: Registration,login and authentication unit
a. Match username and Password

b. Login, move control to dashboard

Step 3: Patient Diseases Filing or detailed description of disease.
a. Update the system diseases
b. Fill the form
c. Upload to database
d. Intimate the selected doctor.

Step 4: Doctor Registration,login and activities
a. Doctor inpatient and outpatient analysis
b. Consultation and diagnose
c. Refer to the lab for detailed diagnosis

Step 5: Decision making

Step 6: Update the patient with latest summaries report.

6. CONCLUSIONS

The system has successfully achieved the system objective as described while processing. The system is also achieved development and simulated environment for patient doctor interaction and communication. The system behavior is analyzed and future online report sharing feature is deployed.

On comparison with other approaches, the overall system is connected via stream of data which has relationships from a doctor to patient. Hence the proposed work can be deploying in cloud for future environment.

REFERENCES

[1]J. Zhou, Z. Cao, X. Dong, X. Lin and A. V. Vasilakos, Securing m-Healthcare Social Networks: Challenges, Countermeasures and Future Directions, IEEE Wireless Communications, vol. 20, No. 4, pp. 12-21, 2013.

[2]J. Sun, Y. Fang and X. Zhu, Privacy and Emergency Response in EhealthcareLeveraging Wireless Body Sensor Networks, IEEE Wireless Communications, pp. 66-73, February, 2010.

[3]J. Li, M.H. Au, W. Susilo, D. Xie and K. Ren, Attribute-based Signature and its Applications, In ASIACCS'10, 2010.

[4] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, SAGE: A StrongPrivacy-preserving Scheme against Global Eavesdropping for EhealthSystems, IEEE Journal on Selected Areas in Communications, 27(4):365-378, May, 2009.

[5]. F. Cao and Z. Cao, A Secure Identity-based Multi-proxy Signature Scheme, Computers and Electrical Engineering, vol. 35, pp. 86-95,2009.