International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 12 – SEPTEMBER 2017.

Cloud-Based Privacy of Patient's And Healthcare Review

J.Nirmala[#1], M.Leena Christy[#2] and A.Prabhu Chakkaravarthy[*3]

[#] *Department of CSE, PG Student, St. Joseph's College of Engineering, Chennai*

[*] *Assistant Professor, Department of CSE, St. Joseph's College of Engineering, Chennai*

***Abstract*— Cloud computing is emerging as a promising technology for computing and it is drawing attention from both academia and industry. Organizations use the cloud in a variety of different service models with such as SaaS, PaaS, and IaaS and deployment models private, public, hybrid, and community. According to a current Cloud Security Alliance report, insider attacks are the sixth biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background authorizations are conducted for personnel who have physical access to the servers in the data center. The cloud-computing model shifts the computing infrastructure to third-party service providers that manage the hardware and software resources with significant cost reductions. It is emerging as a new computing technology in the medical sector besides other business domains. Huge numbers of health administrations have started shifting the electronic health information to the cloud environment. Storing the medical data in cloud will handle the treatment efficient by retrieving patient's medical history from the database before going for the treatment and get to know about the health issues of the patient. And also for security all the data encrypted and then only it will be store in server. During emergencies doctor can only view the details but cannot update. Our project mainly focuses on the issues of security concepts over cloud and manages the medical data of each individual. Existing systems store the data of only a particular organization or group of organizations but not to all hospitals our system will ease the patient to access their health records from cloud. This leads to overhead to the public who wishes to change their doctor of hospital for which the person need to go through all the medical inspections again.**

***Index Terms*— Authentication; access control; security and privacy; distributed cloud computing; m-healthcare system.**

I. INTRODUCTION

A system which handles the medical history of each registered individuals and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered. The details of the patients will be stored and a reference number will be generated when their data are stored into the database for the first time after the implementation of the system. The reference number is used as a unique code to access the database. Whenever they go for a treatment, their medical data will be stored into the database using their reference number. For security reasons, any person who wants to view their data will be allowed only to read the data. They will not be given access to update the database. For hospitals to update the database they require the reference number along with the one time password that generatedto the person whose record has to be store.

II. RELATED WORKS

PSMPA: Patient Self-controllable and Multi-level Privacy preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System[1]distributed medical healthcare (m-healthcare) cloud computing which facilitate efficiently in patient treatment for medical consultation by sharing personal health information among healthcare providers. However, it brings about the challenge which keeps both the data confidentiality and patients identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be straight forwardly exploited. To solve the problem, a novel authorized accessible privacy model (AAPM) in this paper is established. Patients can permit physicians by setting an access tree supporting flexible threshold predicates. Then, based on it, by devising a new method of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative validation scheme realizing three levels of security and privacy requirement in distributed healthcare cloud computing system is proposed. The directly authorized doctors, the indirectly authorized doctors and the unauthorized persons in medical consultation can respectively decipher the personal health data and/or verify patient's identities by satisfying the access tree with their own attribute sets. Finally, the formal security proof and simulation effects illustrate our scheme can resist various kinds of attacks and far out performs the previous ones in terms of computational, communication and storage overhead.

Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical System [2] this system uses two clouds for effective securing. Once the data Owner publish the data it will get encrypted and stored in the cloud. The particular which is used more can be called. Example: Java training Company i.e. if we search word relating java only company related to java will give result no other unrelated company. From the document Keyword are extracted for use .These keys stored by encrypting in public cloud data will be stored in encrypted way in private cloud. Sensitive data such as user name, email id, address will be removed so that other person will not know about the person. Key document and word will be stored in public. Data will be

stored in private. ABE is an Attribute Based Encryption Algorithm is used so that only particular data only see the information they want patient disease, test, observation, result. Full history can be viewed for hospital MD if he is doctor for example only MD for commercial purpose can view the expenditure alone. Pharmacist can only see the medicine when have given to patient similarly others. When file is modified read the content of the document and finds the sensitive data automatically and store in the server (Private cloud).Not sensitive data will be shared in the public. If all data stored in the private means storage will be more. Data automatically identified from system and monitor. Non sensitive data will be put in public cloud. Sensitive data will be put in private cloud. Key is extracted and key is encrypted then stored in private. Normal data encrypted and stored in public. Authentication key is generated. When data query go to public check the relevant data system generate key and data user particular query go to public cloud and check for relevant data and system generate key. Data owner request then requested user if say ok then key authenticated. First public cloud check data and then to private cloud, pass request to enter key to user match using decrypted key and see the data. More secure using key generated algorithm encryption and decryption key is used. If encrypted key match decrypted key then only data can be viewed.

Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption [3] personal health record is used to exchange patient's information it is often outsourced to be stored at a third party, such as cloud providers. However there has been wide privacy as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacyis guaranteed simultaneously by exploiting multi authority ABE. Our scheme also enables dynamic modification of access policies or file attributes efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results show the security, scalability, and efficiency of our proposed scheme.

An Ambient-Aware Elderly Monitoring System [4] the increasing number of elderly population at home and abroad necessitates enhanced approaches to elderly care provision. Elders, often with cognitive and physical impairment, want assistance in their activities of daily living (ADLs), which is usually provided by human caregivers (HCGs). As the demand for caregiver's assistance growths, the shortage of traditional care resources becomes obvious. In this paper, we present the Virtual Caregiver (ViCare) framework that supports a HCG to monitor continuously the elderly by being aware of their surroundings. The ViCare system attempts to recognize the elderly persons' activities and contexts based on the data captured by the sensors placed in their environment and dynamically decides what services to afford them or whether there is a need to interfere HCG depending on the kind of activities. It not only minimizes the cognitive load of the HCG but also delivers a seamless assistance to the elderly toward their improved health and well-being in their active environment. We conducted the experiments in an instrumented household environment and obtained positive results in terms of the satisfaction of the elderly, interaction event handling, caregiver's acceptance, and their commitment.

Cross-domain Data Sharing in Distributed Electronic Health Record System [5] cross-organization or cross-domain cooperation takes place from time to time in Electronic Health Record (EHR) system for necessary and high-quality patient treatment. Cautious design of delegation mechanism must be in place as a building block of cross-domain cooperation, since the cooperation inevitably involves exchanging and sharing relevant patient data that are considered highly private and confidential. The delegation mechanism grants permission to and restricts access rights of a cooperating partner. Patients are unwilling to accept the EHR system unless their health data are guaranteed proper use and disclosure, which cannot be easily achieved without cross-domain authentication and fine-grained access control. In addition, revocation of the delegated rights should be possible at any time during the cooperation. In this paper, we propose a secure EHR system, based on cryptographic constructions, to enable secure sharing of sensitive patient data during cooperation and preserve patient data privacy. Our EHR system further incorporates advanced mechanisms for fine-grained access control, and on-demand revocation, as enhancements to the basic access control offered by the delegation mechanism, and the basic revocation mechanism, respectively. The proposed EHR system is demonstrated to fulfill objectives specific to the cross-domain delegation scenario of interest.

III. EXISTING SYSTEM

Cloud based health systems mainly focused on collecting, storing, accessing, analyzing, and presenting the patient's details. The current techniques are time consuming, inefficient, laborious. It is also obvious that currents technique is violating the real time data access for monitoring the patients. A private cloud server is provided among distributed health care providers. However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patients personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering. Thus the disadvantages are less security, time

consuming, and transport large volume of reports with data confidentiality.

IV. PROPOSED SYSTEM

Cloud based health system is a distributed computing system, where a pool of virtualized and dynamically-scalable services are delivered. This system provides an environment where patient's records are stored and it will be referenced by the doctors to improve the efficiency of the treatment. Thus it handles the medical history of each individual and provides access to all registered hospitals to view and update the data through a reference number. The details of the patients will be stored and reference number will be generated at the first time of registration. For security reasons, registered persons are only allowed to view their data. They are not allowed to update their data. To update, each hospital require their reference number along with their password. Thus the advantages are achieving data confidentiality, providing privacy with high efficiency, overcomescomputational and communication overhead, avoid large volume of data and provide safety.

V. METHODOLOGY

There are four modules used in this proposed system. They are:

1 Online registration and emergency case
2 Accessing patient's details
3 Patient Feedback and Rating
4 Admin View

A. METHODOLOGY DESCRIPTION

1) ONLINE REGISTERATION AND EMERGENCY CASE

The hospital will register here and then they will add the doctor with doctor details. After registration the doctor will get the user name and password through mail. Next the hospital will add the patient details through registration process thus patient will get user name and password based on their attributes. By using this user name and password the patient can log-in to this application.Alert message comes when any person uses their user-name and password. If the patient is unconscious the doctor can get the health records of the patient by using the patient's thumb image which was given by the patient during the registration.

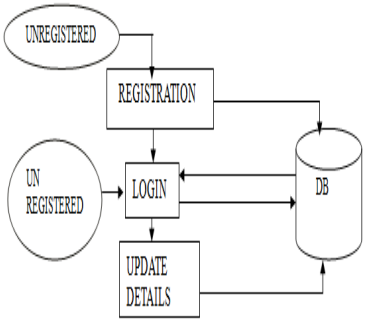

Fig1. Online registration and Emergency case

2) ACCESSING PATIENTS DETAIL

The hospital member will do the appointment for the patient to doctor. In this appointment, the hospital member will root this patient to the doctor based on their problems which was given by the patient. Once the appointment was given by the hospital to the patient then only the doctor can view that appointment details and also he can view the patient problem. The doctor have to type one time password which is generated in his mail when he select the patient's appointment and also the patient have to tell their one time password which have been generated when the doctor fix the appointment. If both onetime passwords get matched only the doctor can view and update the patient's records.

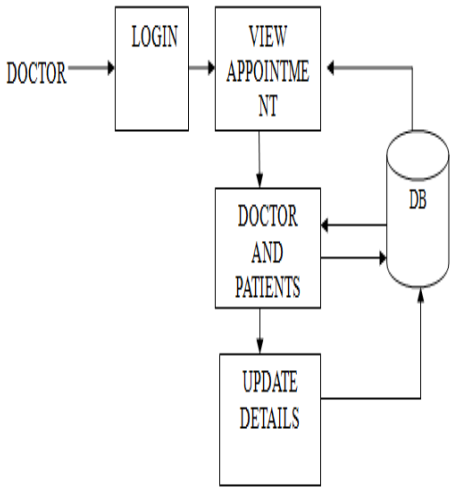

Fig2. Accessing patient's detail

3) PATIENT'S FEEDBACK AND RATING

After the appointment with doctor, If the patient want to give feedback about the doctor patient have to login through their user-name and password can give a feedback about that doctor. The patient cans also give feedback of the doctors whom they have visited and patients can write a feedback about doctors.

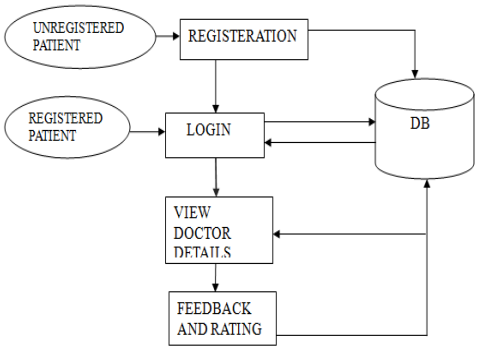

Fig3. Patient's feedback and rating

4) ADMIN VIEW

Admin will manage the registration and also view the feedback and ratings about the doctor given by the patient. He will analysis the data given by the patient through dual technique. Thus the specialist doctor can be found by the patient's rating and feedback will be viewed by admin and rating will be generated.

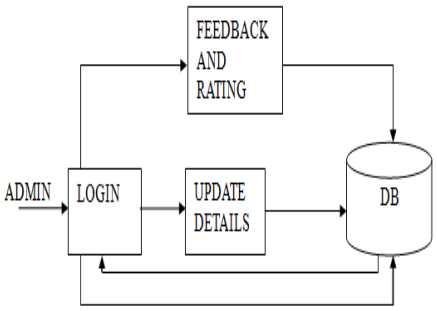

Fig 4. Admin View

VI. ALGORITHM

A. *ABE algorithm :*

begin

1. Attributes are collected.
2. First two letter of each individuals are grouped.
3. AES is used to encrypt these grouped attributes.
4. Password is generated.

end

OTP Generation Algorithm:

begin

1.Attributes are collected.

2.Rijndael algm=Left shift and right shift

3.Shifting for n times.

4.OTP will be generated and sent to mail.

end

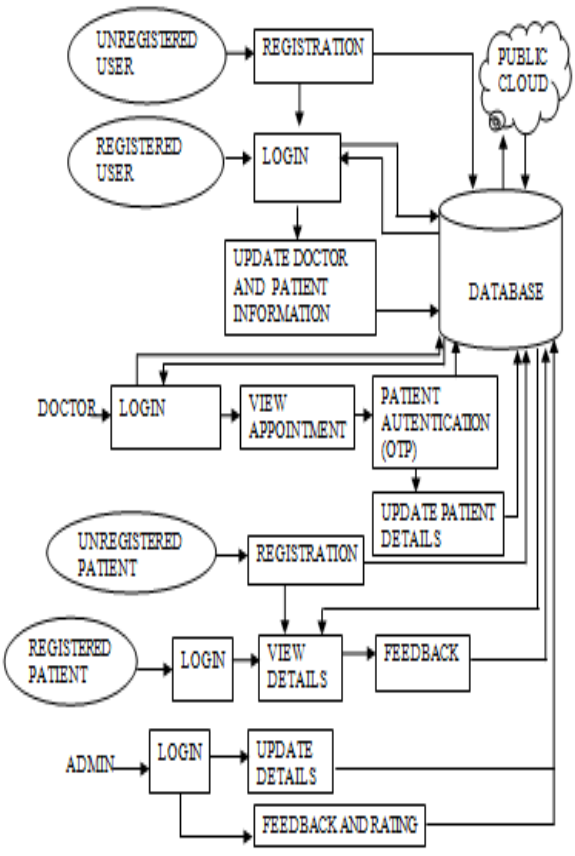

Fig5. System Architecture

VII. CONCLUSION

Thus we monitor the health care details of each individual of the country. It promises to increase the speed in which applications are deployed, increase innovation at lower costs, all while increasing business agility. To the new generation of cloud based health system, cloud computing is better approach in the future. To ensure high efficiency of the proposed framework, we have presented and analysed the key challenges that need to be solved in order to develop efficient and secure patient-centric monitoring system. This concise survey paper is expected to serve as the design for our work is based on a better understanding of the root causes leading to the failures of existing security and privacy preservation schemes for health monitoring.

REFERENCES

[1] Zhou, Jun, Xiaodong Lin, Xiao lei Dong, and Zhenfu Cao. "PSMPA: Patient Self-Controllable and Multi Level Privacy Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System." Parallel and Distributed Systems, IEEE Transactions on 26, no. 6 (2015): 1693-1703.

[2] Mitchell, Robert, and Ing-Ray Chen. "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. “Dependable and Secure Computing, IEEE Transactions on 12, no. 1 (2015): 16-30.

[3] Li, Ming, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption." Parallel and Distributed Systems, IEEE Transactions on 24, no. 1 (2013): 131-143.

[4] Hossain, Md Aynal, and Dewan T. Ahmed. "Virtual caregiver: an ambient-aware elderly monitoring system." Information Technology in Biomedicine, IEEE Transactions on 16, no. 6 (2012): 1024-1031.

[5] Sun, Jinyuan, and Yuguang Fang. "Cross-domain data sharing in distributed electronic health record systems." Parallel and Distributed Systems, IEEE Transactions on 21, no. 6 (2010): 754-764

[6] Jorge Calvillo, Student Member,IEEE, Isabel Roman, Sergio Rivas, and Laura M. Roa, Fellow, IEEE,”Privilege Management Infrastructure for VirtualOrganizations in Healthcare Grids”,VOL. 15, NO. 2, MARCH 2011.