Healthcare Monitoring system using Cloud computing

Shanthakumar Palanisamy[1], Karuppusamy Dhandapani[2], Prakash Mahalingam[3], Arunkumar Dhanabal[4]
[1] *Professor, V. S. B Engineering College, Karur, TamilNadu- 639111.*
[2]*karuppusamydr@gmail.com,* [3]*prakashm731997@gmail.com,* [4]*arunkumardbtech@gmail.com, UG Scholars, V. S. B Engineering College, Karur, TamilNadu- 639111.*

Abstract— **In the fast growing world, healthcare improvements and innovations are unavoidable one. The Electronic Health Record (EHR) is a longitudinal collection of electronic health information stores the patient's data. The healthcare information system is to maintain the information about the every patient and consulting physician's prescriptions for the diseases. In existing system the Clinical Document Architecture (CDA) developed to core document standard to ensure the patients details and prescriptions recommended by the doctors. Fortunately, hospitals are managing the huge volume of patient's information according to rapid growing of population is risky. Now a day world's patients ratio increasing and everyone wants to live in a longer periods, because to maintain the details regarding the patients is a mandatory one. A conflict rises also when more hospitals start using the CDA document format because the data scattered in different documents are difficult to manage. Our proposed method is to maintain the patient's information and physicians details using the cloud. To maintain the large number of patient's medical records, cure patient's information's to reduce the costs through the use of cloud computing. The specific information is extracted using the One Time Password (OTP) mechanism from the data rich environment like cloud and provide the information about history of the disease and how it can be solved. This will be happened by using the decision support system implementation for health care with the use of software that aids in the process of decision-making in order to ensure the correct diagnosis of the disease. The proposed system consists of the cloud storage to maintain the patients, physician's information and the cloud server control to act based on the request from patients. Patients request based OTP is generated to review the patients prescriptions and treatment stages. The system consists of a data collection layer with a unified standard, a data management layer for distributed storage. The medical diagnosis of an illness can be achieved in many ways, from the patient's description, physical examination and laboratory tests also conducted to identify the severity of the disease.**

Keywords **—Cloud Computing, Electronic Health Record, Patients, One-Time Password, Clinical Document Architecture.**

I. INTRODUCTION

Cloud computing is defined as storing and accessing the data's over the internet. This mechanism will support to access clients via internet. It has consists of three types of services. First one is platform as services, second is Infrastructure as services and the final one is Application as service. Platform as service is defined as the base of service in cloud computing, it allows developing, running and managing the applications for clients. Software as service is defined as software that is used to manage huge volume database. Infrastructure is another type of service is that allows the user to remotely use hardware and resources on pay per use model. It is also known as hardware as service. Cloud computing is emerging a new computing paradigm in the healthcare sector besides other business domains. Large numbers of health organizations have started shifting the electronic health information in to the cloud environment. Introducing the cloud services in the health sector not only for the exchange of electronic medical records among the hospitals and clinics also enables the cloud to act as a medical record storage center. Moreover, moving to the cloud environment provides to the healthcare organizations for infrastructure management and also reduces the development and maintenance costs. Apart from this, storing the patient health data in the third party servers also is not achieved the privacy and security. So probable declaration of medical records stored and swapped in the cloud, the patients' privacy concerns should essentially be considered when design the security and privacy mechanisms.

Various approaches have been used to preserve the privacy of the health information in the cloud environment. This survey aims to encompass the

state-of-the-art privacy- protecting approaches employed in the e-health clouds. Moreover, the privacy-preserving approaches are classified into cryptographic and non-cryptographic approaches and taxonomy of the approaches is also presented. Furthermore, the strength and weaknesses of the presented approaches are reported and some open issues are highlighted. The electronic health record is the record of patient's medical history, that maintained by provider over time. It also includes all clinical data of patient like progress notes, medications, past medical history, laboratory and radiology reports, etc. The important one of the users is patient. The patient has authority of the personal records. They only are desire records going to doctor see. The OTP means One Time Password. That is the temporary password code. It generated by an algorithm and it used for authenticating to access of medical records. The Clinical Document Architecture defines the structure of certain medical records like discharge summaries, progress notes, exchange this information between providers and patients, etc. It means the Clinical Document Architecture gives the overall works of the process.

II. LITERATURE SURVEY

Min Chen et al. [1] explain the LIVES include data collection, emotion recognition, and result validation, as well as emotion feedback. We adopt transfer learning to label and validate moods in LIVES, while the emotion can be classified into six types of mood in a reasonable accuracy. Through transfer learning, the time-consuming and labor-intensive processing cost on data collection and labeling can also be greatly reduced. In our prototype system, LIVES are used to enhance an emotion-aware robot's intelligence provided by cloud. LIVES-based emotion recognition is executed in the remote cloud while corresponding result is sent to the robot for emotion feedback.

Cyber data consist of call, SMS, email, application usage and Wi-Fi and network control. Social network data include SNS content or image post, repost and comment. Then, the data are preprocessed. After preprocessing, we extract the data feature. For the emotion space, the data are labeled and validated by transfer learning based on previously labeled results.

Min Chen et al. [2] delivers kind of computation offloading benefits compute-intensive applications, the corresponding service models and analytics tools are remaining open issues. In this paper we categorize computation offloading into three modes: remote cloud service mode, connected ad hoc cloudlet service mode, and opportunistic ad hoc cloudlet service mode. We also conduct a detailed analytic study for the proposed three modes of computation offloading at ad hoc cloudlet. We categorize computation offloading into three modes: Remote Cloud Service (RCS), Connected ad hoc Cloudlet Service (CCS), and OCS.

In the design spectrum, the OCS mode can be treated as an intermediate mode between CCS mode and RCS mode, thus yielding more flexibility and cost effectiveness to enable a more energy-efficient and intelligent strategy for computation offloading through the use of an ad hoc cloudlet.

Min Chen et al. [3] gives the experimental results conducted by OPNET verifies the viability of NDN and adaptive streaming to support the healthcare services involving the transmissions of rich media contents between WBAN and internet. When the physiological information collected in WBAN is distributed to cloud computing platform, a new healthcare service mode is enabled by ''cloud-assisted WBAN, where user's body signals can be stored, processed, managed and analyzed over a long-term period. Though the provisioning of healthcare services is largely enhanced via cloud-enabled technologies, more challenging issues are raised due to the increased user's requirements on Quality of Experience (QoE) in terms of user mobility, content delivery latency, and personalized interaction. To the best of our knowledge, there is no other research investigating the overlay of NDN on top of WBAN until now. In a dynamic and unstable wireless environment, NDN with adaptive streaming is a suitable solution to support the mobility of both patients and physicians.

Jiafu Wan et al. [4] exposes an application scenario regarding the context-aware dynamic parking services by illuminating the cloud-assisted architecture and logic flow. This leads to an increasing evolutionary tendency to change from vehicular networks toward cloud-assisted context-aware vehicular cyber physical systems. In this article, we first propose a multi-layered context-aware architecture and introduce two crucial service components, vehicular social networks and context-aware vehicular security. The seamless integration of vehicular networks and MCC provides tremendous opportunities for VCPS. We provide a brief review and outlook of this promising field, and discuss a cloud-assisted context-aware VCPS architecture for vehicular networks.

Jiafu Wan et al. [5] delivers study a cloud-enabled WBAN architecture and its applications in pervasive healthcare systems. We highlight the methodologies for transmitting vital sign data to the cloud by using energy-efficient routing, cloud resource allocation, semantic interactions, and data security mechanisms with efficient management of the large number of

monitored data collected from various WBANs is an important issue for their large-scale adoption in pervasive healthcare services. Since WBANs have limited memory, energy, computation, and communication capabilities, they require a powerful and scalable high-performance computing and massive storage infrastructure for real-time processing and data storage, as well as for online and offline data analysis.

The seamless integration of WBANs and MCC provides tremendous opportunities for pervasive healthcare systems. We provide a brief review and outlook of this promising field, and discuss a cloud-enabled WBAN architecture for pervasive healthcare systems.

Kwangsoo Lee Thomas et al. [6] produces hospital industry had experienced an economic crisis in 2008, and they are facing another financial crisis in 2011. These economic crises have precipitated the decline in hospital resources. They are required to balance the productivity for providing healthcare services and satisfying the need of people. The study included 577 hospitals in the statistical analysis. The HIS was measured by three indicators, which is based on the number of application systems in three core hospital functions (administration, management, and clinical). American Hospital Association and Dore fest IHDS were merged to create sample data. Structural equation modeling was applied to estimate the parameters of the model. HIS is negatively associated with the total expense. However, it was not statistically significant.

This study found that HIS measuring by the information system applications had relationship with the reduced total cost. Although the relationship was not statistically significant, this result implied that hospitals investing more resources for IS could lower cost for providing healthcare services.

Min Chen et al. [7] it *c*ompared to the conventional healthcare system, a wearable computing-based solution is advantageous in many ways by upgrading the healthcare model from the traditional on-spot mode to in-home mode. Wearable body sensor devices might cause patients to feel uncomfortable, which further incurs stress and unhealthy emotions. The provisioning of healthcare services can be significantly enhanced via wearable enabled technologies; great challenges arise due to the lack of a human-centric mechanism for affective interaction. In this article, we propose a novel architecture, Affective Interaction through Wearable Computing and Cloud Technology (AIWAC), which includes three components: collaborative data collection via wearable devices, enhanced sentiment analysis and forecasting models, and controllable affective interactions. Hybrid emotional data analysis is which support computation- intensive analysis of various emotional data from CPS- Spaces. Dynamic resource perception and allocation is which provides users with real-time, available, and effective affective interaction.

Md. Golam Rabiul Alam et al. [8] gives human brain chemistry changes over different mental disorders but still causes and effects are not fully explored. And pinpointing the location of mental disorder in our brain is very difficult as our brain consists of about 100 billion neurons and glial cells, and the neurons form the telecommunications network in the brain to communicate each other and also carry the signals back and forth between your brain and the rest of your body. A suicide risk scouting is prototype by predicting mental states in cloud environment. In this system, patients' real-time vital diseases symptoms are collected through Wireless Body Area Network (WBAN) and then analyzed the collected data in healthcare cloud platform with patient's historical repository of diseases, habits, rehabilitations and genetics. Here, the mental statuses of patients have been modeled as the discrete set of states of Hidden Markov Model (HMM), where WBANs annotations and stored facts of patients in cloud are considered as the observations of HMM. Predicting mental states using some tiny sensors and cloud computing technology is a novel initiative to monitor patients of suicide risk and of some mental disorders. It supports to prevent some undesirable and unwanted live loosing.

Min Chen [9] delivers in the past decade RFID systems have been incorporated into a wide range of industrial and commercial systems, including manufacturing and logistics, retail, item tracking and tracing, inventory monitoring, asset management, anti-theft, electronic payment, anti-tampering, transport ticketing, and supply-chain management. The intrinsically passive features of existing RFID systems, to which we refer as first-generation RFID systems, render their adaptation to real-world dynamics in order to efficiently comply with up-to-date application specific requirements difficult. To address this challenging issue, we propose an evolution to second-generation RFID systems characterized by the introduction of encoded rules that are dynamically stored in RFID tags. This novel approach facilitates the systems' operation to perform actions on demand for different objects in different situations, and enables improved scalability. We have discussed the many benefits that our proposed 2G-RFIDSys can provide, including improvements in system scalability, information availability, automated monitoring and processing of sensitive information and access control and claim that these benefits can be achieved by employing RFID tags

with more memory to encode information- rich data along with action scripts that can be interpreted by the corresponding subsystems to automate a number of processes.

Varun Chandola et al. [10] experts agree that inefficiencies in the current healthcare system, healthcare delivery. We translate the problem of analyzing healthcare data into some of the most well-known analysis problems in the data mining community, social network analysis, text mining, and temporal analysis and higher order feature construction, and describe how advances within each of these areas can be leveraged to understand the domain of healthcare. Our main contribution is the translation of some of key challenges faced by the healthcare industry as knowledge discovery tasks. The three case studies presented in this paper attack the problem of identifying fraudulent healthcare providers in three independent ways, using state of art KDD methodologies, which have never been previously used in this context.

III. PROPOSED SYSTEM MODEL

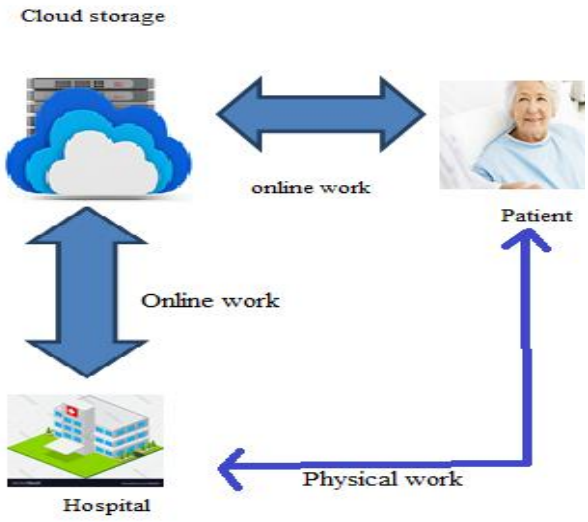

Fig.1 Outline of the healthcare system using cloud

The proposed system for cloud is used in healthcare systems. That uses the public cloud and provides the OTP security for the patient‘s information. This consist that five stages named as hospital admin, apply the attribute based encryption for PHR doctor maintain for PHR, secret key generation and deploy in cloud environment. In this project uses fine-grained and scalable data access control for PHRs, we leverage Homomorphism- Based Encryption (HBE) techniques to encrypt each patient’s PHR file. PHR system is divided into multiple security domains that greatly reduce the key management complexity for owners and the users. We conceptually divide the users in the system in to types of domains namely public and personal domains (PSD). In the public domain, we use multi authority HBE (MA- HBE) to improve the security and avoid key escrow problem. It overcomes the past disadvantage and the advantages are we are use public cloud, and the key escrow problem and we use homomorphism- based encryption. It also have OTP security mechanism to provide security with provide end to end communication such as doctor and patient. The patient is going to choose which files the doctor going to see , so it reduces the physical work. The cloud storage is used for storing both patient records and hospital data like doctors details. The patient is sign up the account in cloud. And also the doctor is creating the account via admin. That means the admin create account for doctor with the id and password. The patient request the appointment date and time from the doctor and patient upload the files of patient past medical records. The creation of account and get the appointment from the doctor is use the way of internet. But before the appointment the doctor need to see the patient medical records at the time the OTP is generated and send to the doctor. After the appointment the patient meet the doctor directly in appointed date and time.

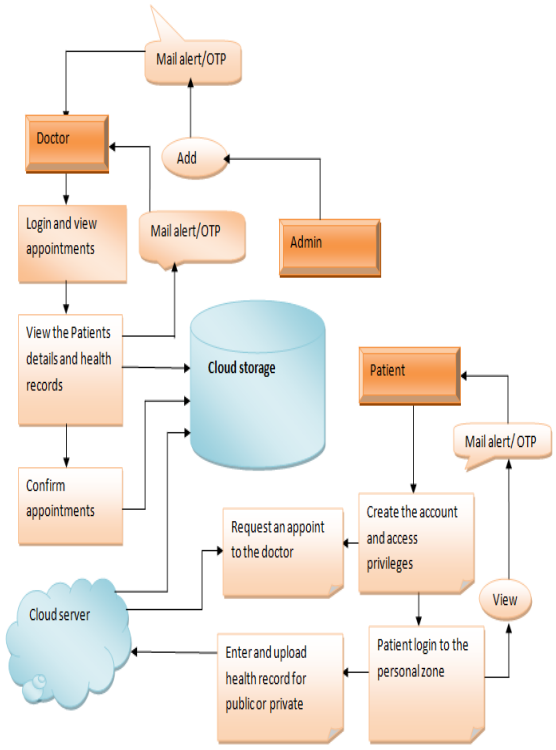

Fig.2 Over all process of the system

3.1) Hospital admin:

The hospital admin is responsible for the doctor details. The admin have four tasks. They are add doctor, view doctor, delete doctor and log out.

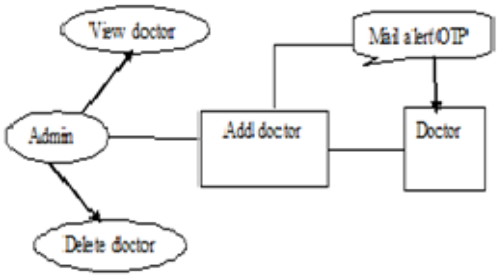

Fig.3 Admin process

3.1.1) Add the doctor:

Admin is the only responsible for adding the doctor in the database. The hospital admin to create the account for Doctor and the account consists of following information details of following Doctor Name, Id, Email id, hospital name, specialist, mobile number and Password. The Password will be providing through the mail to Doctor, why because using this mail alerts process means avoid fake doctors' login process.

3.1.2) View doctor:

It has the all doctors details of admin included. The doctor's details are shown in list manner.

3.1.3) Delete doctor:

The field of delete doctor requests the doctor id. The id is the unique for every doctor. so the doctor data is deleted using this id.

3.2) Patient login:

It shows the patient log in form. This is also contains the new user sign up form with reset password. The patient log in form requires the details of patient name and password.

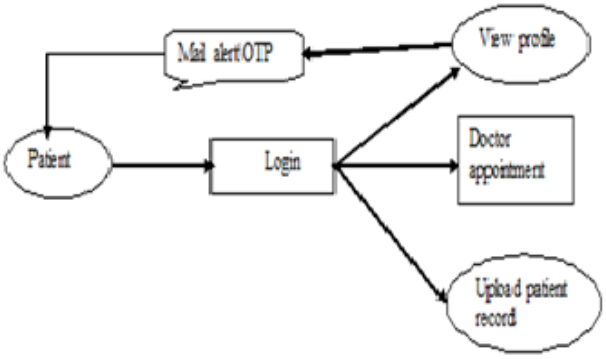

Fig.4 Patient Process

3.2.1) New user:

While create the account for new user the following details are requires such as user name, full name, password, conform password, date of birth, blood group, gender, address, mail id and mobile number.

3.2.2) Reset the password:

The reset password page requires the user name, current password and new password. That changes the old password as new password.

3.3) Doctor login:

Doctor login the his account name with the password what admin gave and sent to the doctor mail.

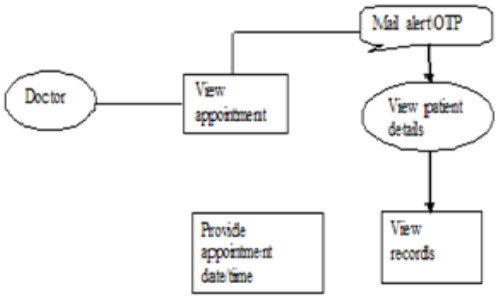

Fig.5 Doctor Process

3.4) Apply the attribute based encryption for PHR:

Personal health information could be exposed to those third party servers and to unauthorized parties so we want to secure the PHR .in this part we are using attribute based encryption to protect the PHR information.

3.5) Doctor maintain for PHR:

Doctor to view the patient PHR information and give the Appointment Date and Timing for the corresponding patient and this details only access the authorized patient and his gave the privileges friends or relatives.

3.6) Secret key generation:

The patient wants to know about the status of the PHR first search the record and the corresponding secret key will be automatically mail to the authorized patient mail id .after enter that secret key to access the PHR file information.

3.7) Deploy cloud environment:

Finally we are deploying this application in cloud environment. Why we are deploying cloud environments means to reduce the bottle neck problem and any ware any time we can access our information and real time insert, delete, and update our record to the cloud environment.

IV. RESULT AND DISCUSSION

Consider this project, there are three persons are involved .They are Admin, Patient and Doctor. The Admin manage the hospital data. That means adding or appointing the doctors and managing the doctor's data with create the account in cloud for every doctor with the id and password. The next person is patient. The patient creates the account in cloud for storing

the health records. Another one person is doctor. He receives the patient appointment request messages and views the history of health records. We use the public cloud to store the patient health records. This is not in secure manner. So, we use the OTP for the security. The patient is send what are the files view by doctor. When the doctor views the files at a time the One Time Password is send to the patient mobile. The patient fills the more than one phone number when the signup the account in cloud. If the patient gives the permits the doctor via OTP then the doctor views the record otherwise no.

It reduces the use of physical records and it reduces the cost of cloud storage because we going to use the public cloud. That is basically less secure compared to the private cloud. So we provide the OTP security.

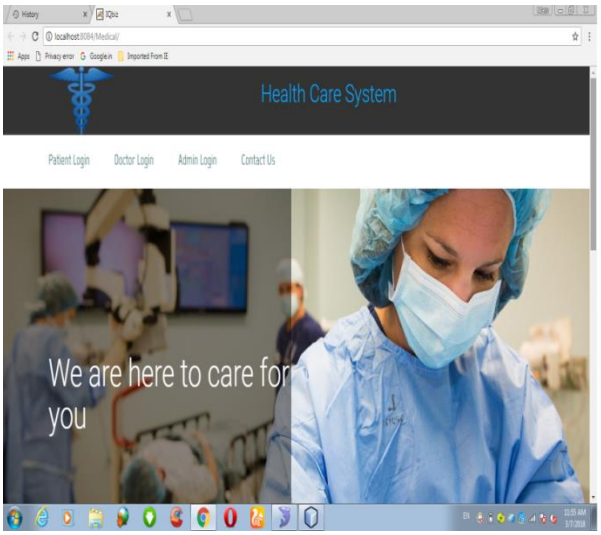

Fig.6 Initial Page

The website is initially has an above fig.6. It shows the patient login, doctor login, admin login and contacts details.

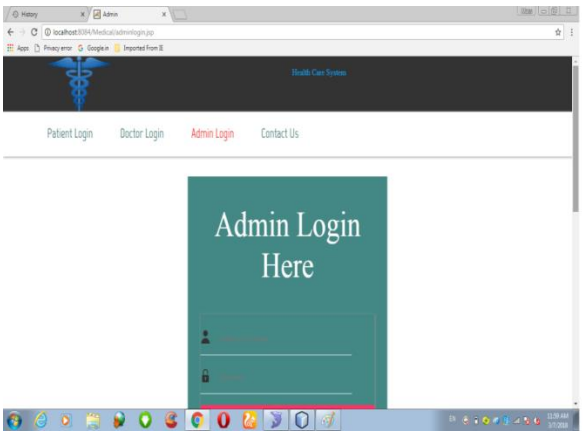

Fig.7 Admin Login page

The admin login page requires the admin name and password for the authentication. And the admin have an authority for adding, deleting and viewing the doctor.

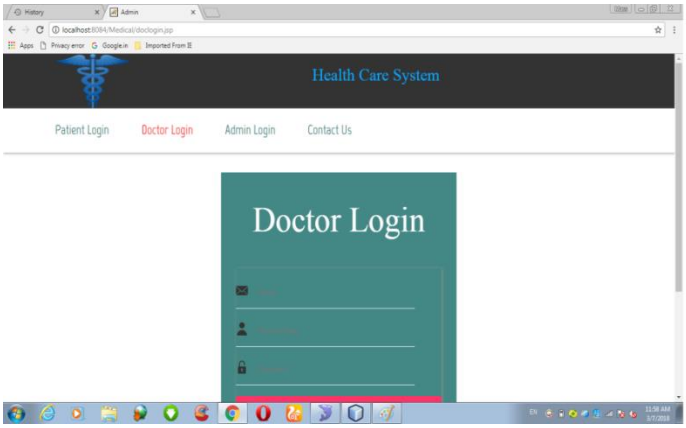

Fig.8 Doctor Login Page

The doctor has separate login page. It requires the name, id and password. That password is send to the doctor mail when admin create the account for the doctor in cloud.

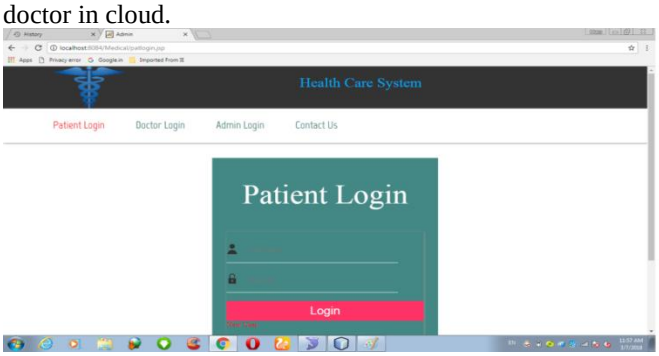

Fig.9 Patient Login Page

The patient login page requires the patient name and password. This also have new user account creation link.

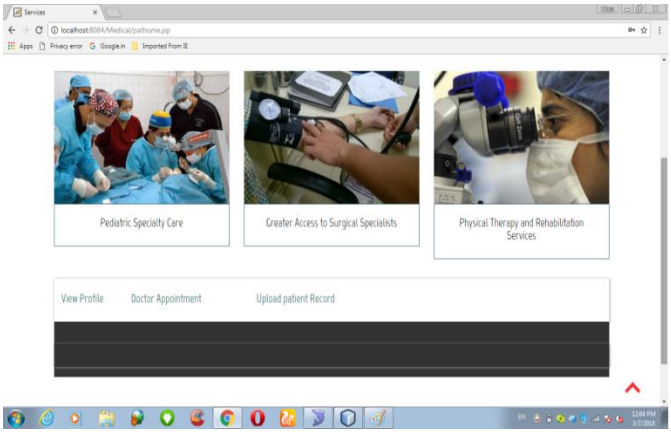

Fig.10 Patient Appointment Page

The patient requests the appointment from the doctor with the following actions. Upload the past history medical records from cloud and view the available doctors in particular hospital and view the profile of owns.

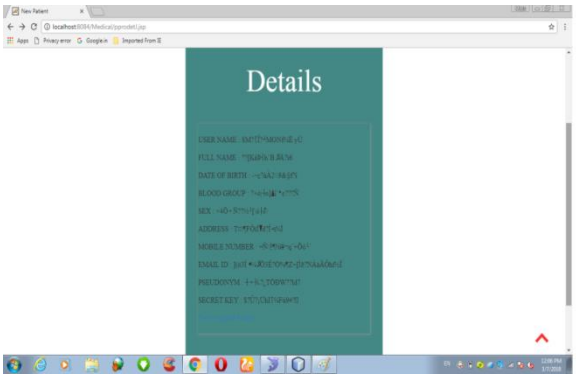

Fig.11 Encrypted Information's

The patient or doctor request to view the record or details at the time the data or information is shown in the encrypted manner. And below of record have an link of view the original details. When click on that link, the OTP is generated and send to patient or doctor mail id. It secures the data or information of patient. And also it gives another one advantage is it uses the public cloud as private cloud, so reduce the cost.

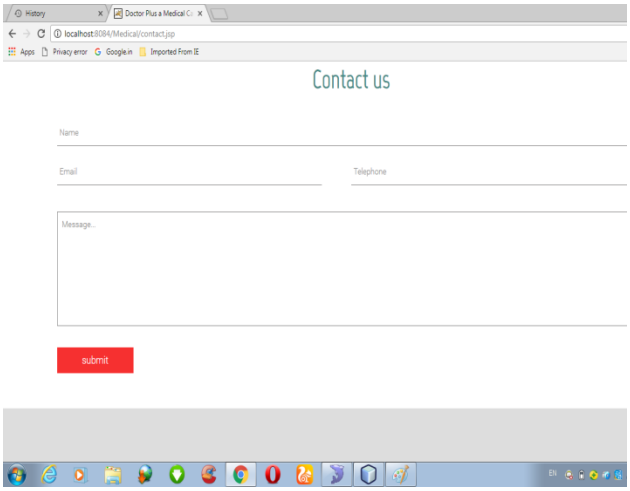

Fig.12 Contact Details

The final page having the hospital contact details. It used for identify the hospital city and address with the telephone contacts.

V. CONCLUSION

We have proposed a novel framework of secure sharing of individual health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework provides the individual dares brought by many PHR holders and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations. Also, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient.

VI. FUTURE WORK

We note that, although using ABE and MA-ABE rises the system extendibility, there are some restrictions in the virtually of using them in building PHR Systems. For example, in workflow-based access control scenarios, the data access right could be given based on users' identities rather than their attributes, while ABE does not handle that efficiently. In those scenarios one may consider the use of attribute-based broadcast encryption (ABBE) . In addition, encrypt or access policy is somewhat limited by that of MA-ABE's, since it only supports conjunctive policy across multiple AAs. In practice, the credentials from different organizations may be considered equally effective, in that case distributed ABE schemes will be needed. We designate those issues as future works.

VII. REFERENCE

1) M. Chen, Y. Hao, Y. Li, D. Wu, and D. Huang, "Demo: LIVES: Learning through interactive video and emotion-aware system," in Proc. ACM Mobihoc, Hangzhou, China, Jun. 22–25, 2015.
2) M. Chen, Y. Hao, Y. Li, C. Lai, and D. Wu, "On the computation offloading at ad hoc cloudlet: Architecture and service models," IEEE Commun. Mag., vol. 53, no. 3, pp. 1–7, Jun. 2015.
3) M. Chen, "NDNC-BAN: Supporting rich media healthcare services via named data networking in cloud-assisted wireless body area networks," Inf. Sci., vol. 284, pp. 142–156, Nov. 2014.
4) J. Wan, D. Zhang, S. Zhao, L. T. Yang, and J. Lloret, "Context-aware vehicular cyber-

physical systems with cloud support: Architecture, challenges, and solutions," IEEE Commun. Mag., vol. 52, no. 8, pp. 106–113, Aug. 2014.

5) J. Wan et al., "Cloud-enabled wireless body area networks for pervasive healthcare," IEEE Netw., vol. 27, no. 5, pp. 56–61, Sep./Oct. 2013.
6) K. Lee, T. T. Wan, and H. Kwon, "The relationship between healthcare information system and cost in hospital," Pers. Ubiquitous Comput., vol. 17, no. 7, pp. 1395–1400, Oct. 2013.
7) M. Chen, Y. Zhang, Y. Li, M. Hassan, and A. Alamri, "AIWAC: Affective interaction through wearable computing and cloud technology," IEEE Wireless Commun. Mag., vol. 22, no. 1, pp. 20–27, Feb. 2015.
8) M. G. R. Alam, E. J. Cho, E. Huh, and C. S. Hong, "Cloud based mental state monitoring system for suicide risk reconnaissance using wearable bio sensors," in Proc. 8th Int. Conf. Ubiquitous Inf. Manage. Commun., 2014, p. 56.
9) M. Chen, S. Gonzalez, Q. Zhang, M. Li, and V. Leung, "A 2G-RFID based E-healthcare system," IEEEWirelessCommun. Mag., vol. 17, no. 1, pp. 37–43, Feb. 2010.
10) V. Chandola, S. Sukumar, and J. Schryver, "Knowledge discovery from massive healthcare claims data," in Proc. 19th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2013, pp. 1312–1320.