

Medical Assistance System

Agrani Nehra¹, Aditya Bhadange², Muzammil Khan³

¹ Student, Information Technology, MET Bhujbal Knowledge City, Maharashtra, India

² Student, Information Technology, MET Bhujbal Knowledge City, Maharashtra, India

³ Student, Information Technology, MET Bhujbal Knowledge City, Maharashtra, India

ABSTRACT

Healthcare spending has led to an increase in calls for ways to reduce the cost of healthcare. Amidst the debate on the best approach on cut costs in the healthcare system, one of the few bipartisan provisions is the need to integrate modern technology into the storage and transfer of medical records. Current attempts to establish such electronic medical records are challenged by concerns about patient privacy, issues with the incorporation of old records, and budget limitations. We propose the development of personal portable healthcare record smart cards and a corresponding framework to simplify maintenance and transfer of patient records as an incremental step towards a nationalized electronic records system. This system is a feasible and cost-effective system that applies existing technology to address inefficiencies of the traditional paper approach for medical records system; simultaneously, it also serves as a transition system to facilitate the adoption of completely electronic medical records.

Keyword - MAS.

1.INTRODUCTION

During the second half of the 20th century, the national expenditure on healthcare[1] increased dramatically. Indeed, India spends on average six times as much per capita compared to other industrialized nations on healthcare administration. The need to cut down on the costs of healthcare is widely acknowledged. Despite this urgent need, past efforts to reduce the amount of spending such as managed care organizations, perspective payment systems, and payment per capita have only elected temporary or marginal change. Policymakers are investigating other approaches to mitigate the cost of healthcare, including increased privatization, drug price regulation, and modernized medical record keeping[2]. Of these proposals, adopting electronic medical records systems is widely favoured as a solution to reduce expenditures, and studies suggest they also increase efficiency, minimize medical errors, and improve patient satisfaction.

In general, physicians who use electronic records report high levels of satisfaction. It is reasonable therefore to investigate how government policy can aid healthcare providers in transitioning to electronic medical records. Automation systems in hospitals serve the purpose of providing an efficient working environment for health care professionals. Access to accurate health data quickly is one of the main functions of this system. There can be many sources that the information related to the patients can be obtained from the patient, test results, doctor diagnoses for patient illness, health measurement devices and previously stored patient information. The usual way of obtaining relevant data is from paper record. The Paper-based records have a low cost and have limitations such as difficult to access, time-consuming to update, secure, impossible to share and maintain for lifelong. The problems can be solved by increasing the capabilities of hospital automation systems by using intelligent storage and retrieval mechanism. Smart card can play a key role in sharing patient specific information. The patient can carry the health smart card with him/her anywhere and anytime and present it to the doctor at the time of consultation. Smart cards are more suitable to use in health care information systems because of they are cheap, easy to use, carry and update with new information and should not get damaged easily. Smart cards can be described as portable integrated devices that

store and process data. These tiny computers with their own memories and processors have a widespread usage especially in telecommunication and mass transit systems. Speed, security and portability properties make smart cards a potential tool in healthcare systems. Many countries implement or continue to develop such systems including smart card components.

The objective of the present work is to develop a multifunctional user- friendly biomedical measurement device[1] of an Integrated Electronic Health Record System, which provides a complete e-record in place of paper record. The following health parameters are required by any doctor such as Blood Pressure, Blood glucose level measurement, pulse oxygen meter, clinical analyzer. Each device was designed, built, tested and calibrated separately. The modules devices are connected serially to a Personal Computer with a Visual Basic software package. The data acquired from each system is then displayed on the PC monitor and store data in Health Smart card. With the beginning of the Web 2.0 era, the internet began growing up and developing with tremendous speed. Many opportunities, such as sharing knowledge, information, and opinion with other users, came out. This did, favor the development of social networks like Facebook.

Nowadays, authors can share their creations with millions of readers around the globe. Amateur-musicians can get famous faster than ever before just with uploading their tracks. Business world have found more customers and profit in the internet. The variety of online shops, auctions or ea markets opened up in the internet. Today, every user of the World Wide Web can purchase almost any item being in any country of the world. As opposed to real shops, in the internet there are no place-limitations. In fact, there is almost endless place. Nevertheless people came across a new problem in the WWW. The amount of information and items got extremely huge, leading to an information overload. It became a big problem to and what the user is actually looking for. Search engines partially solved that problem, however personalization of information was not given. So developers found a solution in recommender systems. Nowadays the amounts of information we are retrieving have become increasingly enormous. Back in 1982, John Naisbitt observed that: we are drowning in information but starved for knowledge. This "starvation" caused by having many ways people pour data into the Internet but not many techniques to process the data to knowledge.

2. LITERATURE SURVEY

In a paper by authors Sherin Sebastian et. al., gives a picture based procedures to procure and investigate a steady gushing of ECG flag through computerized camera for picture catching, data extraction and examination performed utilizing MATLAB instruments and additionally information sending framework in light of web system [1]. The strategy catches the imperative signs and parameters from the ICU checking machine utilizing a webcam and transmits the picture through the web. This unique picture is then benefited to the counseling specialist by means of an ANDROID phone. If there should arise an occurrence of oddity a warning is send to the specialist's telephone. The paper proposed a strategy to catch, think about and produce caution with respect to the patient's condition utilizing the heart rate and make the picture be accessible to the doctor.

Distributed storage is these days extremely prominent capacity framework. Distributed storage is putting away of information off-site to the physical stockpiling which is kept up by outsider. Distributed storage is sparing of computerized information in legitimate pool and physical stockpiling traverses various servers which are overseen by outsider. Outsider is in charge of keeping information accessible and open and physical environment ought to be secured and running at record-breaking. Rather than putting away information to the hard drive or whatever other nearby stockpiling, we spare information to remote stockpiling which is available from anyplace and at whatever time. It diminishes endeavours of conveying physical stockpiling to all over the place. By utilizing distributed storage we can get to data from any PC through web which discarded restriction of getting to data from same PC where it is put away [2]. While considering information protection, we can't depend on customary method of verification, in light of the fact that surprising benefit acceleration will uncover all information. Arrangement is to scramble information before transferring to the server with client's own key. Information sharing is again imperative usefulness of distributed storage, since client can share information from anyplace and at whatever time to anybody. For instance, association may concede consent to get to some portion of delicate information to their representatives.

However, difficult assignment is that how to share encoded information. Customary way is client can download the scrambled information from storage, unscramble that information and send it to impart to others, however it loses the significance of distributed storage. Cryptography system can be connected in a two noteworthy ways-one is symmetric key encryption and other is uneven key encryption. In symmetric key encryption, same keys are utilized for encryption and unscrambling. By differentiation, in deviated key encryption distinctive keys are utilized, open key for encryption and private key for decoding [3].

2.1 Key Aggregation System

Information sharing is a fundamental common sense in distributed storage. In this article, we tend to demonstrate an approach to immovably, perseveringly, and adaptably impart information to others in distributed storage. We tend to depict new open key cryptosystems which fabricate consistent size figure writings indicated prudent designation of cryptography rights for any arrangement of figure writings are potential [4]. The curiosity is that one will blend any arrangement of mystery keys and fabricate them as conservative as one key, however encompassing the office of all the keys being aggregative. In various words, the key holder will unleash a steady size mix key for flexible choices of figure content set in distributed storage, yet the inverse encoded records outside the set remain classified. This minimized mix key might be conveniently sent to others or be hang on terribly accuse account credit of extremely confined secure stockpiling. We give scholastic security investigation of our plans inside the typical model. We furthermore portray diverse use of our plans. Particularly, our plans give the essential open key patient-controlled encoding for adaptable pecking order that was in any case to be known. File Terms: Cloud stockpiling, information sharing, key-total encryption, persistent controlled encryption.

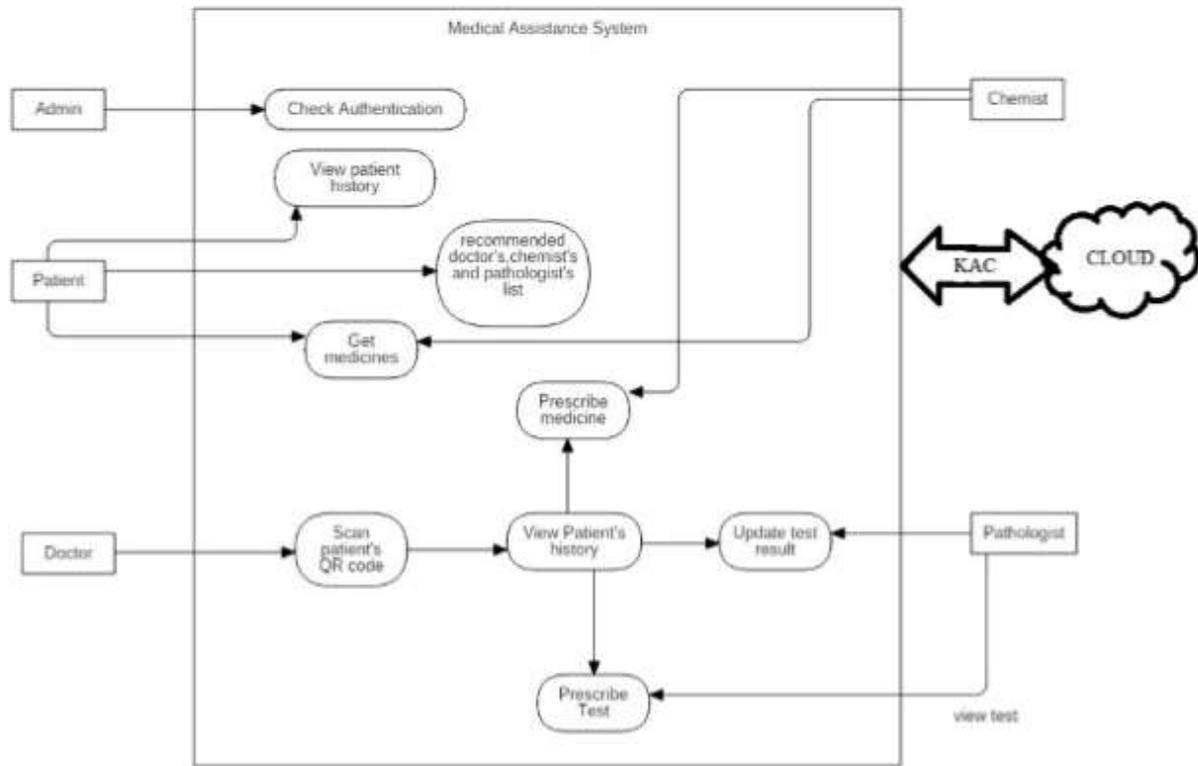
Cloud has turned out to be vital in web world. Cloud gives stockpiles, stages which enhances the usefulness. Distributed storage demonstrates how safely and adapt ably we can store and share our information [5]. This strategy presents a unique kind of encryption called as key-total cryptosystem which permits client to share their information incompletely crosswise over cloud and which produces steady size cipher text. In this strategy client give a consistent size total key for various cipher text classes in distributed storage, yet the other encoded documents outside the class stay classified. We additionally contrast this method and existing one. We executed this cryptosystem for open key patient-controlled encryption framework.

Cloud assumes the essential part in web world. Cloud gives stockpiles, stages which enhances the usefulness. Distributed storage indicates how safely and adapt ably we can store and share our information. With the assistance of keys client can without much of a stretch and safely share their information over cloud. This presents Key Aggregate Cryptosystem in which a total key is made utilizing which client can share their information halfway over cloud and it gives a steady size cipher text. Notwithstanding conventional cryptographic key era procedures, this method has extraordinary cryptographic key total cryptosystem which is useful for secure cloud and protection safeguarding key era prepare. We propose get to level arrangement structure, for example, Public and Private Access level to enhance the information get to component in the information sharing cloud instrument prepare. We are utilizing calculation, for example, Blowfish calculation which brings about higher security and speedier execution when contrasted with AES (Advanced Encryption standard) and DES (Data Encryption Standard). Likewise the blowfish calculation is unpatented and no permit is required[6].

3. PROPOSED SYSTEM

All the users/patients have aadhar card with them at this point of time. The aadhar card already contains some basic information of the user/patient which makes it easy for creating a new account over the cloud. The users (admin,patient, doctor, chemist, pathologist) can login through the end user application for MAS. After selecting the type of user, the QR code from Aadhar Card is scanned for verification. The patient has to scan the QR code on the aadhar card through our system which identifies if the user is new or existing. If the user is new, he has to create an account and store all his medical health records. If the user is existing, he can upload new health records. Past records and new updates can be fed into the system but cannot be directly modified. Our system also recommends information about top k hospitals and doctors in the nearby area which makes it efficient and less time consuming. The patients can also rate the doctors and hospitals they have visited in the past years. This data is collected from all the users/patients and list on top k doctors and hospitals is created. This list of top k doctors/hospitals is based on

the users location. Doctors can access only those records of patients he is treating or treated over the past years. The doctor and patient can access the cloud based medical history details as per the assigned rights. Modifications can only be done through a combined access for the doctor and patient together.



MAS: System Workflow

4. CONCLUSIONS

Here in Medical Assistance system it presents information about the algorithms used, Key Aggregation Cryptosystem and provided diagrams for the system. The use of aadhar card makes the system accessible and friendly for all, as each and every individual already possesses an aadhar card. In case of emergencies, this system would play a vital role as the basic details of the patient can be easily retrieved which can help give proper treatment to patient. Every kind of user logs in to the system and accesses Medical records as per the rights. Our system could be more efficient and less time consuming as it doesn't require users to carry medical records. In case of misplacing the records, our system could be helpful. Our system recommends top doctors and hospitals which could make the user easier to make decision regarding health.

5. REFERENCES

[1]. Sherin Sebastian, Neethu Rachel Jacob, Yedu Manmadhan, Anand V. R. , M. J. Jayashree, "REMOTE PATIENT MONITORING SYSTEM", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.5, September 2012, pp. 99-110

[2].Balaji M, Rajashekar S A, " Data Sharing in Cloud Storage Using Aggregate Key Cryptosystem", International Journal of Computer Science Trends and Technology (IJCT) – Volume 3 Issue 2, Mar-Apr 2015, PP.172-176

[3].Aruna Kumara B, 2AravindaThejas Chandra," Secured Data Sharing In Cloud through Key Aggregation",International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 5, May 2015,pp.4185-4186.

[4].Imtiaz Ahmed," DATA SHARING IN CLOUD STORAGE USING KEY-AGGREGATE CRYPTOSYSTEM", International Journal For Technological Research In Engineering Volume 3, Issue 2, October-2015,pp.179-182.

[5].Rashmi Khawale,Roshaniade," Patient Controlled Encryption using Key Aggregation", International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 21, April 2015,pp.29-31.

[6].Rashmi Khawale,RoshaniRaut(Ade)," Patient Controlled Encryption using Key Aggregation with Blowfish Algorithm", International Journal of Computer Applications (0975 – 8887) National Conference on Advances in Computing (NCAC 2015),pp.11-14.

