A Multimedia Based Hybrid System for Healthcare Application using Attribute Based Encryption

Vaishali Dhawas[1], Hanumant Raut Mali[2], Swapnil Harde[3], VishalBarage[4]

Department of Computer Engineering,
Sinhgad Institute of Technology,
Lonavala, Maharashtra, India.

[1]vnd.sit@sinhgad.edu, [2]rauthanumant@gmail.com, [3]swapneil99@gmail.com, [4]vishalbarage@gmail.com

***Abstract*—Healthcare field is one of the most advanced fields today but it still needs some convergence. Primary healthcare and secondary healthcare services are provided all over the world but the gap between doctors and patients needs to be bridged. The systems available in the market provide a static interface for the communication between patient and doctor. The communication is simply text type and verbal communication. This type of interactions is not clear and efficient between doctors and patients.With the advancement in technology, the other file types such as images, audio and videos can also be used for communication. Multimedia plays an important role in such cases. Our goal here is to design a multimedia hybrid system which will help converge all communication methods and file types for better communication between doctors and patients. This will provide a single platform for all communication for doctors and patients. This system will not just be accessible through desktops and laptops but also through mobile devices. This will make it a multimedia hybrid system.**

I. INTRODUCTION

Today, there are many applications over the web that can be used to improve the appointment system i.e. a patient can go online and take an appointment. But these systems just provide a static interface which has only text, radio buttons and check boxes which can be used to take an appointment and cancel an appointment [1]. What if a patient wants to communicate more with a doctor? The goal of system is to bridge this gap between a doctor and a patient and provide a system through which a doctor and a patient can communicate better and during different frames of time and that too more frequently.

As per w3school's definition [3], "Multimedia comes in many different formats. It can be almost anything like text, images, voice, video, animations and more." Therefore, use of multimedia can be really useful for healthcare application because it gives you a chance of interacting with more real time data. For example, a child has fallen while playing and is badly wounded then after sending a video of it the doctor can instruct first aid till driving the child to hospital.

After an investigation on healthcare applications in the current market, we found that there is no healthcare application which provides complete solution to doctors and patients. Also the communication mechanism is text type and verbal communication. This type of interactions is not clear and efficient between doctors and patients.

Our goal here is to design a multimedia based hybrid system which will help converge all the communication methods and file types for better communication between doctors and patients. This system will provide a single platform for the clear communication for patients and doctors. This system will not just accessible through desktops and laptops but also through mobile devices. This will make it a multimedia hybrid system [1]. This idea is to bring different people and devices together through multimedia for better communication to have a better healthcare system. All the users will be provided with the system which can be deployed over any server and can be accessed through an application provided to the particular user.The system will provide an interface to a patient through which he can see all the details and communicate with the doctor as well. Another interface will be provided to doctor through whom he can see patient's details and provide prescription to the patient. This will automatically reduce time and effort along with providing flexibility between doctors and patients.

II. RELATED SYSTEMS IN HEALTHCARE

There are two types of applications already being developed in this field viz, first is web applications and the other is mobile applications. Let us understand them one by one.

A. HealthVault

It is a software product from Microsoft. One gets a free account here which basically includes sharing of personal health records with many web applications, family members, friends and others [1][4]. It simply provides a static interface for the users to communicate with each other. Some drawbacks of HealthVault were such as the user did not have the write access control and the user was not able to decide his key for encryption. The

user was not able to share his personal health records with his family members, friends and others. HealthVault user interface is shown below [4].

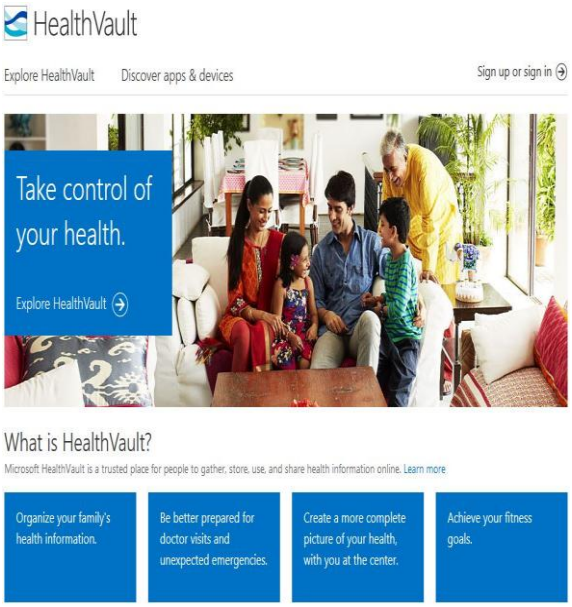

Fig.1 HealthVault [4]

B. *Kaiser Permanente*

Kaiser Permanente provides various facilities along with a good interface for the patients and doctors [5]. A patient can book an appointment with the doctor online which further gets approved by the doctor. A patient here can also communicate with the doctor through email. The main drawback of Kaiser Permanente was that sometimes there was no clear communication between doctor and patient due to no clear idea of the patient's health to the doctor. Kaiser Permanente user interface is shown below [5].

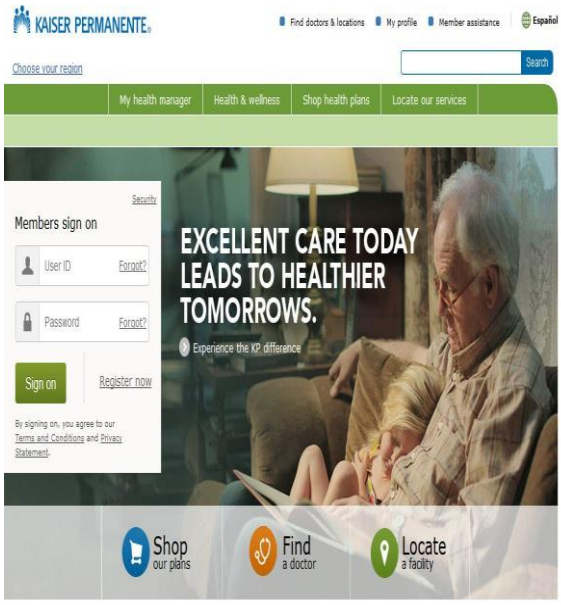

Fig. 2 Kaiser Permanente [5]

C. *Curas*

Curas basically is a mobile application developed for iPhone OS [1][7]. With Curas a user can perform various functions such as scheduling appointment, view labs and imaging tests. Curas was the first mobile healthcare application developed for iPhone OS. The user interface for Curas is shown in the figure shown below [7].

Fig. 3 Curas [6]

D. *Haiku from Epic Systems*

Haiku is a mobile application provided by Epic Systems which provides a good interface for the users to handle their electronic health records, clinical schedules, health summaries, test results and notes through secure access [1][8]. It simply provides a static interface where the patient is provided a list of symptoms and he is supposed to select appropriate ones.

Then the doctor has to give the prescription according to the symptoms being selected by the patient. In this system the main problem was that sometimes doctor was not able to get clear idea about the patient's healthwhich leads to various misunderstanding between them.There was no clear and efficient communication between patient and doctor which finally leads to some misunderstanding between doctor and patient. So sometimes wrong prescription might be given from doctor to patient.The user interface provided by Epic Systems for Haiku is shown in the figure shown below [8].

Fig. 4 Haiku from Epic Systems [8]

III. PROPOSED WORK

As we are developing two applications i.e. one for desktop/laptops and other for mobile phones [1].Two different technologies are used to develop the two distinct applications.

System architecture for desktop/laptop application is shown below.

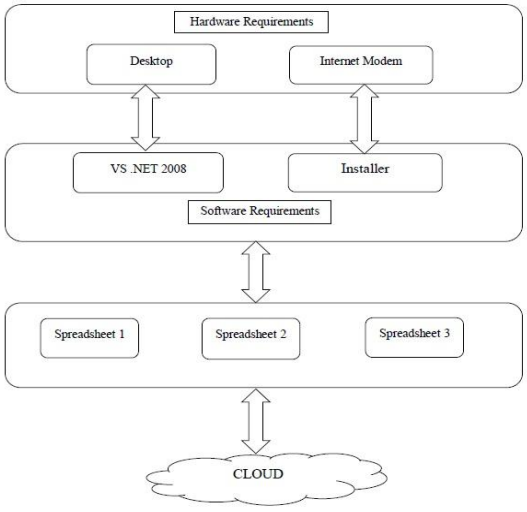

Fig. 5 System Architecture for Desktop/Laptop Application

System architecture for mobile phone application is shown below.

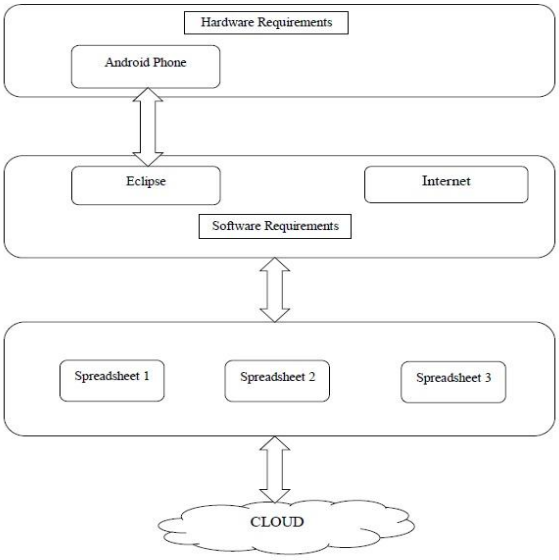

Fig. 6 System Architecture for Mobile Phone Application

Desktop application is provided with the full version of the system where as the mobile application is provided with the small version of the system. The following kind of users can access the system:

1. **Admin**: Admin can add new doctors and patients to the system. Doctors and patients need to request admin for system access.
2. **Doctor**: Doctor can view images and videos uploaded by all the patients and provide prescription to the patients. Doctor can access all the appointments for the current day and manage them.
3. **Patient**: Patient can upload images and videos to the particular doctor and get the prescription. Patient can add an appointment according to the time slots available for a particular doctor.

A. Mobile platform to use:

A very important million dollar question is that which mobile platform should our application be developed for? According to our survey 79% of the smartphone owners had an Android OS device, 14.2% had an Apple iOS device and Blackberry claimed 2.7% of the market share [10]. The complete breakdown is indicated in the diagram below.

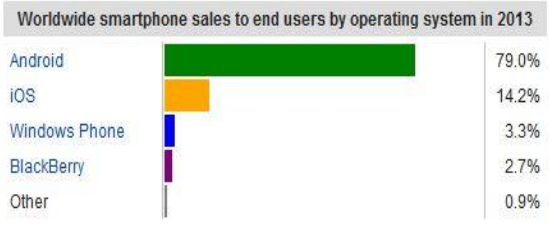

Fig. 7 Mobile OS market share [10]

IV. ALGORITHM

A. *AES:*

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U. S. National Institute of Standards and Technology (NIST) in 2001. Originally called Rijndael, the cipher was developed by two *Belgian* cryptographers, Joan Daeman and Vincent Rijmen, who submitted to the AES selection process. The algorithm described by AES is a symmetric-key generation algorithm, meaning same key is used for encryption and decryption.

B. *ABE Algorithm:*

Cloud computing is a model for enabling ubiquitous, convenient and on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. There are two main categories of cloud infrastructure: public cloud and private cloud. To take the advantage of public clouds, data owners must upload their data to commercial cloud service providers which are usually considered to be semi trusted, that is, honest but curious. That means the cloud service providers will try to find out as much secret information in the users outsourced data as possible, but they will honestly follow the protocol in general[11].

Traditional access control techniques are based on the assumption that the server is in the trusted domain of the data owner and therefore an omniscient reference monitor can be used to enforce access policies against authenticated users [12]. However, in the cloud computing paradigm this assumption usually does not hold, and therefore these solutions are not applicable.

Data encryption is the most effective in regard to preventing sensitive data from unauthorized access. A new concept introduced is Attribute Based Encryption (ABE) algorithm to deal with the security concerns.

Attribute Based Encryption (ABE) is an expansion of public key encryption that allows users to encrypt and decrypt messages based on user attributes. In a typical implementation, the size of the cipher text is proportional to the number of attributes used during decryption. ABE is a new cryptographic primitive which provides a promising tool for addressing the problem of secure and fine grained data sharing and decentralized access control [12].

Key-policy attribute based encryption (KP-ABE) is an important type of an ABE, which enables sender to encrypt messages under a set of attributes and private keys are associated with access structures that specifies which cipher texts the key holder will be allowed to decrypt. In most existing KP-ABE scheme, the cipher text size grows linearly with the number of attributes embedded in cipher text [13]. In this paper we propose a new KP-ABE construction with constant cipher text. In our construction, the access policy can expressed as any monotone access structure. Meanwhile, the cipher text is independent of the number of cipher text attributes and the number of bilinear pairing evaluations is reduced to a constant [13].In KP-ABE system, cipher texts are labelled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures a policy that specifies which type of cipher text the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents.

V. CONCLUSION

The healthcare system is an advanced system that provides a single platform for the clear communication between patients and doctors. Communication is done through various multimedia files such as video and images which automatically reduces time and efforts along with providing flexibility between doctors and patients. Data uploaded by the patient can be viewed by the doctor and the prescription can be provided to the patient for the same. This system will not be just accessible through desktops and laptops but also through mobile devices. Looking at the market, Android is one of the fastest growing mobile device OS. We made this system for Android mobile devices that helps patients and doctors look at the records and schedule an appointment.

VI. FUTURE SCOPE

The system is only accessible through Android OS which can also be made accessible through all other OS such as Apple iOS, Windows, Blackberry Bata and all others. In this system the communication is through various multimedia such as audio, video, image and text where video conferencing could also be included for efficient communication between doctor and patient. Apart from just communication Personal Health Records can also be maintained for patients to store their health information. Also sharing of PHRs could be done between with friends as well as family members.

REFERENCES

[1]. Weider D. Yu, Akash Panwar, Vikas Dahuja and YogeshGoyal, 14th IEEE Conference, 2012 - "A Multimedia Based Hybrid System for Healthcare Application"

[2]. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, VOL. 24, NO. 1, 2013 - "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption"

[3]. HTML Multimedia, Retrieved Nov, 2013, from https://www.w3schoold.com/html/html_media.asp

[4]. HealthVault website [NOV 2013], Retrieved NOV 2013 from https://www.healthvault.com/in/en

[5]. Kaiser Permanente website [NOV 2013], Retrieved NOV 2013 from https://healthy.kaiserpermanente.org/html/kaiser/index.shtml
[6]. Curas website [NOV 2013], Curas EMR Mobile for iPhone, Retrieved NOV 2013 from https://www.curas.com/home
[7]. Curas website [NOV 2013], Curas EMR Mobile for iPhone, Retrieved NOV 2013 from https://www.curas.net/PRODUCT_EMRMOB.html
[8]. Haiku website [NOV 2013], Haiku from Epic Systems, Retrieved NOV 2013 from https://mobihealthnews.com/6030/epic-systems-launches-iphone-ehr-app-haiku/
[9]. Android Developers, Retrieved DEC, 2013 from https://developer.android.com/sdk/index.html .

[10]. Wikipedia, Retrieved DEC, 2013 from https://www.wiki.org/mobilemarketshare
[11]. Susan Hohenberger and Brent Waters, 2013, -"Attribute Based Encryption with Fast Decryption"
[12]. Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, 2012, - "Attribute Based Encryption for Fine Grained Access Control of Encrypted Data"
[13]. Cheng-Chi Lee, Pei-Shan Chung and Min-Shiang Hwang, International Journal of Network Security, 2013 – "A Survey on Attribute Based Encryption Schemes of Access Control in Cloud Environments"