Information Security and Privacy in Healthcare

Divya Raval[1] & Smita Jangale[2]

[1]Student, I.T Department, V.E.S Institute of Technology, Mumbai, India
E-mail: *divya.raval@ves.ac.in*

[2]Associate Professor, I.T. Department, V.E.S Institute of Technology, Mumbai, India
E-mail: *smita.jangale*@ves.ac.in

Abstract: Cloud computing is appearing as a good prototype for computing and is drawing the attention from both academia and industry. The cloud-computing model is transferring the computing infrastructure to third-party service providers that handle the hardware and software resources with important cost reductions. It is emerging as a new computing example in the medical field apart from other business domains. Many health firms have started moving to electronic health information to the cloud environment. Initiating cloud services in the health sector will not only eases the exchange of electronic medical records between the hospitals and clinics but also enables the cloud to act as a medical record storage center. Besides, moving to cloud environment eases the healthcare organizations from the repetitive tasks of infrastructure management and reduces development and maintenance costs. The medical data stored in the cloud makes the treatment systematic by recovering patient's medical history from the database before going for the treatment and get to know about the health issues of the patient.

Keywords: Attribute-Based Encryption (ABE), DDoS, Personal Health Record (PHR), Health Information Technology (HIT)

I. INTRODUCTION

Computers are now general among almost every aspect of our lives, and in many cases, their introduction brought tremendous benefits. Some tasks were made considerably easier; some were even made possible in the first place such as extensive computational tasks and information search over very large amounts of data. Especially administrative processes and information interchange of large organizations could not function without computers anymore. Computers facilitate these tasks by providing information where it is needed.

A sector that depends very much on information but seems to lag these developments is the domain of healthcare [1]. In terms of computer usage, hospitals even seem to be surpassed by the public administration: a collection of data is mostly done on paper and is hardly fed into a computer system. The little data that does reach a computer system usually stays in isolated, such as a database for lab analysis values.

However, mainly in the healthcare domain, a closer combination of systems and a use of computer-aided data processing could be very helpful. Like almost no other domain, quality of healthcare depends on the accessibility of data. When a clinical decision should be made, all the required information should be available [1]. Integration of Information and Communication Technology (ICT) enables quick feedback, remote monitoring and analysis and above all ensure mobility of individuals across countries.

In current years, personal health record (PHR) has appeared as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in a centralized place through the web, from anywhere and at any time (if they have a web browser and Internet connection), which has made the storage, retrieval, and sharing of the medical information more efficient [2]. Especially, each patient has the full control of her medical records and can effectively share her health data with a wide range of users, including staffs from healthcare providers, and their family members or friends. In this way, the accuracy and quality of care are improved, while the healthcare cost is lowered. At the same time, cloud computing has captivated a lot of attention because it provides storage-as-a-service and software-as-a-service, by which software service providers can enjoy the virtually infinite and elastic storage and computing resources. As such, the PHR providers are more and more willing to shift their PHR storage and application services into the cloud instead of building specialized data centers, to lower their operational cost [2]. For example, two major cloud platform providers, Google and Microsoft are both providing their PHR services, Google Health1 and Microsoft HealthVault2, respectively.

Cloud Computing has appeared as a superior platform for storing, managing and accessing data. Personal Health Records are being stored on clouds for efficient usage. On one hand, there is an opportunity for systematic management of data and on the other, there is the problem of privacy and security. A patient should have control over his health records. For privacy, the data should be encrypted properly. The patient should also have the advantage to grant access to persons only who have the corresponding key. This paper proposes to discuss how PHRs can be made scalable and secure.

Despite a common belief that certain boundaries and security issues of the cloud would hinder the shift; the healthcare industry is taking an initiative to move to these cloud-based platforms [3]. Today many doctors and hospitals are moving towards these clouds to provide better healthcare services to their patients.

II. LITERATURE SURVEY

Healthcare IT support systems are subject to change of development and updates during their life cycle. Cloud computing is the idea of providing a platform for utilizing software and hardware remotely without the need for experienced terminals. The necessity for computer hardware and in-house software, which cost a lot of money to maintain, will be terminated using cloud computing. Thus, the infrastructure of the healthcare IT systems platform will be simplified and more efficient.

Every single data or information is the chief responsibility for the organizations especially in healthcare as it needs to be accessible and secure from unauthorized access. The patient's data was saved on manual files and kept them in safes under physical locks in the near past. Data was secured by considering physical security. After the development in the computer field, organizations shifted from traditional manual systems to computer-based data storage systems. This Computer-based information system saved data on hard drives; tape drives and backup were very frequently taken for recovery of data in case of emergency. Data was secure and systematic as well as effective to manage and retrieve by using these automated healthcare information systems. This model shift required health organizations to depend totally on computer-based information systems [4].

Ming Li (2013) describes a new idea of patient-centric structure and process for data access control to PHRs stored in semi-trusted servers. Attribute-Based Encryption (ABE) method was used to encrypt every patient's PHR file. It exploits authority ABE for the privacy of patients by vital improvements of access policies. Revoking of access policy is not possible at all the instants and the attributes which were known to the user leads to privacy concern.

In Attribute-based encryption [5], the data owner should first describe the attributes based on which the encryption needs to be performed. The number of users in the system doesn't matters. Each attribute has a public key, secret key, and a random polynomial, so different users cannot merge their attributes to recover the data, and different users cannot take away collusion attacks. Only the user who has the authorized attributes can meet the expectations of the access policy to decrypt the data. Practically all key generation schemes used by an authority are existing. Since these strategies contain the authority that just meets the need of private cloud environments, the authority should be removed in the future. In Existing attribute-based encryption the main concern such as key management, scalability, effective policy updates, and efficient on-demand cancellation are non-trivial to solve and remain largely open up-to-date.

A. Attributes Based Encryption (ABE)

Security and access control is the main goal of the Attribute-Based Encryption. It is a public-key (PK) based one too many encryptions that allow users to encrypt and decrypt data based on user attributes. In which the secret key (SK) of a user and the cipher text (CT) are dependent upon attributes (e.g. the country she lives, or the kind of subscription she has).In such a system, the decryption of a cipher text is likely only if the set of attributes of the user key matches the attributes of the cipher text. Decryption is only possible when the number of matching is at least a threshold value. Collision-resistance (An adversary that holds multiple keys should only be access data if at least one individual key grants access.) is crucial security features of Attribute-Based Encryption.

Drawbacks:

The issue with attribute-based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this strategy is restricted in the existing environment because it uses the access of monotonic attributes to control user's access TO the system.

B. Multi-Authority Attribute-Based Encryption:

Multi-authority attribute based encryption scheme uses multiple parties to distribute attributes for users. A Multi-Authority ABE system is composed of K attribute authorities and one central authority. Each attribute authority is also assigned a value dk.

A randomized algorithm which must be used by some trusted party (e.g. central authority). Takes as input the security parameter K. Outputs a public key, secret key pair for each of the attribute authorities(PKa , SKa), and also outputs a system public key and master secret key which will be used by the central authority(PKca , SKca). For Attribute, Key Generation algorithm takes as input the authority's secret key, the authority's value dk, a user's GID, and a set of attributes in the authority's domain AkC and outputs secret key for the user. Encryption is done by a randomized algorithm run by a sender it takes a set of attributes for each authority, a message, and the system public key as input and outputs the ciphertext.

A decryption algorithm run by a user takes a ciphertext as input, which was encrypted under attribute set A and decryption keys for an attribute set Au. Outputs a message M. It allows any polynomial number of unconventional authorities to monitor attributes and distribute private keys and tolerate any number of corrupted authorities. In this model, a recipient is defined not by a single string, but by a set of attributes.

Drawbacks:

The complication in multi-authority scheme required that each authority's attribute set be disjoint.

III. INFORMATION SECURITY IN HEALTHCARE

Information security is the preservation of information and information systems from unauthorized access, use, disclosure, interference, modification or destruction. Information security is attained by ensuring the confidentiality, integrity, and accessibility of information. In health care, and for the purposes of this guide, confidentiality, integrity, and availability mean the following:

Confidentiality–the attribute that electronic health information is not made available or disclosed to unauthorized persons or processes.

Integrity – the attribute that electronic health information has not been modified or destroyed in an unauthorized manner.

Availability – the attribute that electronic health information is accessible and useable upon demand by an authorized person.

In advanced healthcare environments, there is a need for well build infrastructure which decreases time-consuming efforts and expensive operations to obtain a patient's complete medical record and uniformly combine this heterogeneous collection of medical data to distribute it to the healthcare professionals. Electronic health records have been widely acquired to enable healthcare providers, insurance companies and patients to create, manage and access health care information in any situation. All the healthcare industries need to handle more requests with the available resources. The main aim of all the healthcare organization is to grow the number of people getting access to healthcare services [6]. Therefore, day by day the amount of data that need to be stored, managed and updated is increasing in an exponential manner. The healthcare industries desire more computation ability so that the quality of the service increases. Cloud computing increases patient care by providing faster, better, secure and universal services at a lower cost and which meets the requirements of the healthcare sector. Thus, healthcare providers are more willing to move their systems to clouds that can remove the geographical distance barriers among providers and patients [6]. With cloud computing, different doctors can access a patient's health records even if they're a distance apart. These physicians need not have a direct communication to request a transfer of health records. They can just access them through clouds.

A. Benefits of Cloud Computing in Healthcare

There are enormous benefits and advantages upon execution of cloud computing in healthcare industry some of which may include:

1. Mobility of records

In many cases, a person's health information can be needed by two or more health institutions in that case by the implementation of cloud technology a person's health information can be easily synchronized and shared at the same time. Hence this improves physician's ability to provide a better health care to the patients [3]. Thus, by the implementation of cloud technologies; a patient's information is readily available.

2. Speed:

By making use of cloud-based technology and services always enable faster and accurate access to all the important information for the healthcare services providers and the history of their patients.

3. Security and Privacy

By utilizing cloud computing is mainly used for storage of medical records online. With the recent HIPAA update, cloud healthcare service providers are now responsible for HIPAA compliance as healthcare entities they serve. Thus, this comprises of encryption of data and secure backup of this data which contains the health information of a person, then verifying if the data can be easily retrieved, and finally, security can be improved by using permission based and secured database.

4. Reduction of costs

By getting these cloud techniques in healthcare- patients, physicians, other medical organizations experience cost reduction. Since there is no need for these health care institutions and doctors to invest great amounts in hardware infrastructure and their maintenance as these problems are already handled and taken care by the cloud computing providers [3]. According to a recent report by Healthcare Financial Management, says depending on the size and extent of the healthcare organizations the reduction is achieved by utilization of EHR's can amount up to $37 million over the next five-year period.

5. Better patient care:

The ability to provide a combine patient medical record containing patient data from all patient encounters across all operators. These records will be available anywhere and anytime enabling healthcare providers to have a comprehensive outlook of the patient's history and provide the most suitable treatments accordingly.

B. Challenges of E-Health Cloud

No doubt, e-Health Cloud provides a lot of benefits in the industry of health care, but unfortunately, it receives several problems in HIT as well as in cloud computing. Processing and storing of sensitive medical data of patients is a major challenge [4]. The following section describes the issues and challenges of e-Heath Cloud and their proposed solutions.

1. Data/Service Reliability

Cloud service providers need to provide excellent reliability of services over the cloud especially in healthcare industry [4]. Healthcare needs data in the right form as well as cloud services. Unlawful

changes in data and errors in data are not adequate. So cloud must provide data and services without any error.

2. Data Management

E-health cloud needs to assign storage of millions of patient's data. Medical specialist accesses this sensitive data from a different location at the same time [4]. There is a different aspect of data like HD graphics, 3D and audio and video data. To manage this data systematically and provide it when desired, fault tolerant systems/services need to be assured.

3. Flexibility

Depending on the need of different healthcare providers, e-Health Cloud Service provider should can serve accordingly [4]. The services provided by cloud should also be very flexible so that services can be configured depending on user requirements. Additionally, adding new services as need should be accommodated.

4. Availability

The most important requirement for any health care providers is the consistent availability of the services from e-Health Cloud. Healthcare providers cannot continue their functions without the availability of services and patient's sensitive data. Therefore, these services should be consistently available without any disturbances. The main reasons for the failure of Cloud services may involve network failure, software and hardware failure, or security attacks and natural disasters. E-Health Cloud should be proactive and ensure continuity of service in an effective and efficient way. If backed up gradation is required, then services for the healthcare should not be interrupted.

5. Security

Could Service providers keep data, of patients from different healthcare organizations? There is need of strong access control and authorization mechanism to secure this huge and sensitive data. The security standards should be executed so that sensitive data can only be accessible to the right organization. E-healthcare service providers can only be shifted to the cloud if they are guaranteed of their desired security [4]. So, policies and standard as organizations want should be properly implemented by the cloud services provider.

6. Privacy

Many healthcare organizations are uncertain to shift to cloud computing services due to privacy concerns. For e-Healthcare systems, Privacy is one of the major alarms because of the sensitivity of patient's data [4]. Due to the sensitivity of patient records cloud is facing serious privacy issues. Recently United States of America (USA) Intelligence agencies recorded the sensitive information of German chancellor. Now organizations are worried about privacy issues.

IV. FLOW OF PROPOSED SYSTEM

In the proposed system, there will be a web application which consists of admin, patient, and physician. Each of these users has different functionality based upon their role. Like admin of the respective hospitals will be able to active the accounts of patient and physician, upload lab reports which are in encrypted form and able to audit user log. The patient will be able to view lab reports,

book appointments online and if he/she is unsatisfied with the treatment provided by one hospital will be able to migrate to the other hospitals with same login credentials so the burden of remembering various login credentials will be eliminated. The doctor will be able to response to the appointment of patients from various hospitals.

The ECC-based cryptosystems have been successfully applied to healthcare systems. Such a system senses a patient's sensitive data transmits to the hospital database, from which the medical personnel can access the patient's information when necessary to monitor the patient's health condition in a real-time manner. To ensure the patient's privacy, the information needed to be encrypted before being transmitted from the database. After that, he/she can download the data stored in the cloud database or upload data to the database both through the encryption/decryption circuits provided by the ECC integration unit. The terminal device, either a personal computer or a portable device, is used to input or display patients' medical data.

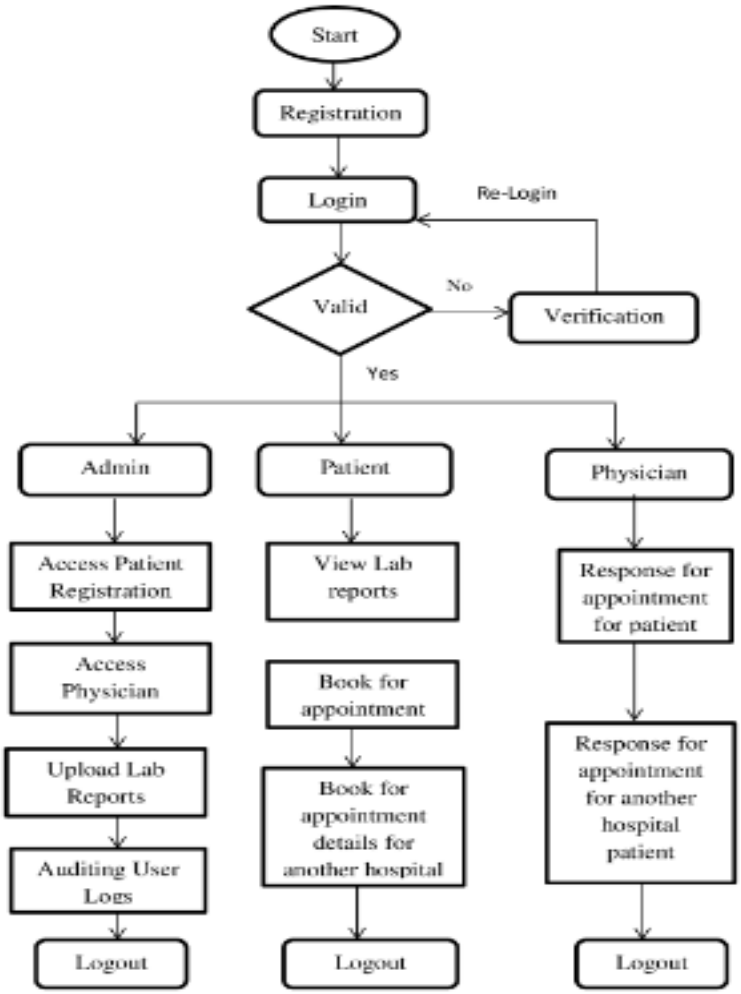

Figure 1: Flow of Proposed System

V. ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM

Elliptic Curve Cryptography is an approach requiring a set of algorithms for key generation, encryption, and decryption for doing public-key cryptography. ECC is based on the mathematics of

elliptic curves developed independently by Victor Miller and Neal Koblitz in 1985-86.ECC as all asymmetric algorithms uses a key pair: one key which is public is used for encryption and another key is the private key which is used for decryption process. The good point about these key pair is that one of these keys cannot be obtained from another key which makes it useful for encryption and decryption process.

Elliptic Curves used in cryptography are typically defined over two types of finite fields: fields of odd characteristics (fp, where p > 3 is a large prime number) and fields of characteristics two (f2m a field of binary bit strings of length m). An elliptic curve is defined in a standard, two-dimensional x, y Cartesian coordinate system by an equation as follows: y2=x3+ax+ b, where a and b are real number constants such that 4a3+27b2 ≠ 0. Elliptic curve groups over real numbers are not practical for cryptography due to the slowness of calculations and round off error [7]. The elliptic curves over finite fields fp of characteristics greater than three can be performed by choosing the variables a and b within the field fp. ECC is based on the difficulty of computing point Q given point P, R and the curve y2 =x3+ax+ b as shown in the figure. The figure gives the basic understanding of how ECC works.

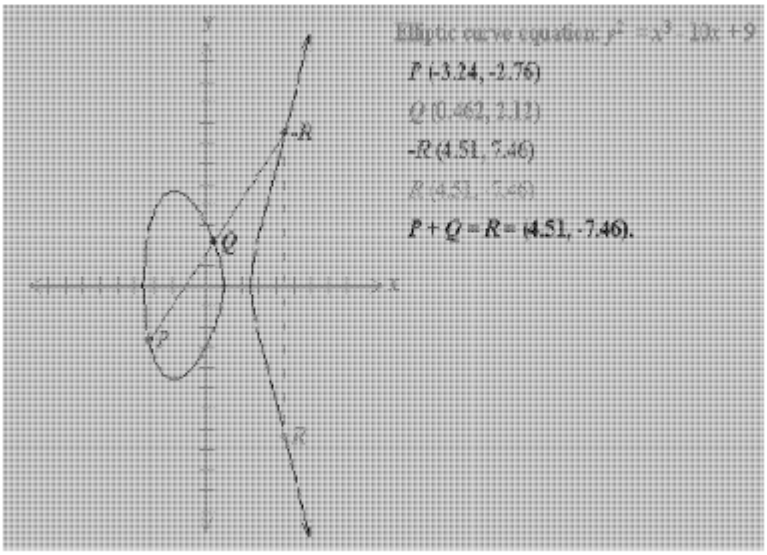

Figure 2: Illustration of Elliptic Curve Cryptography

VI. RESULTS

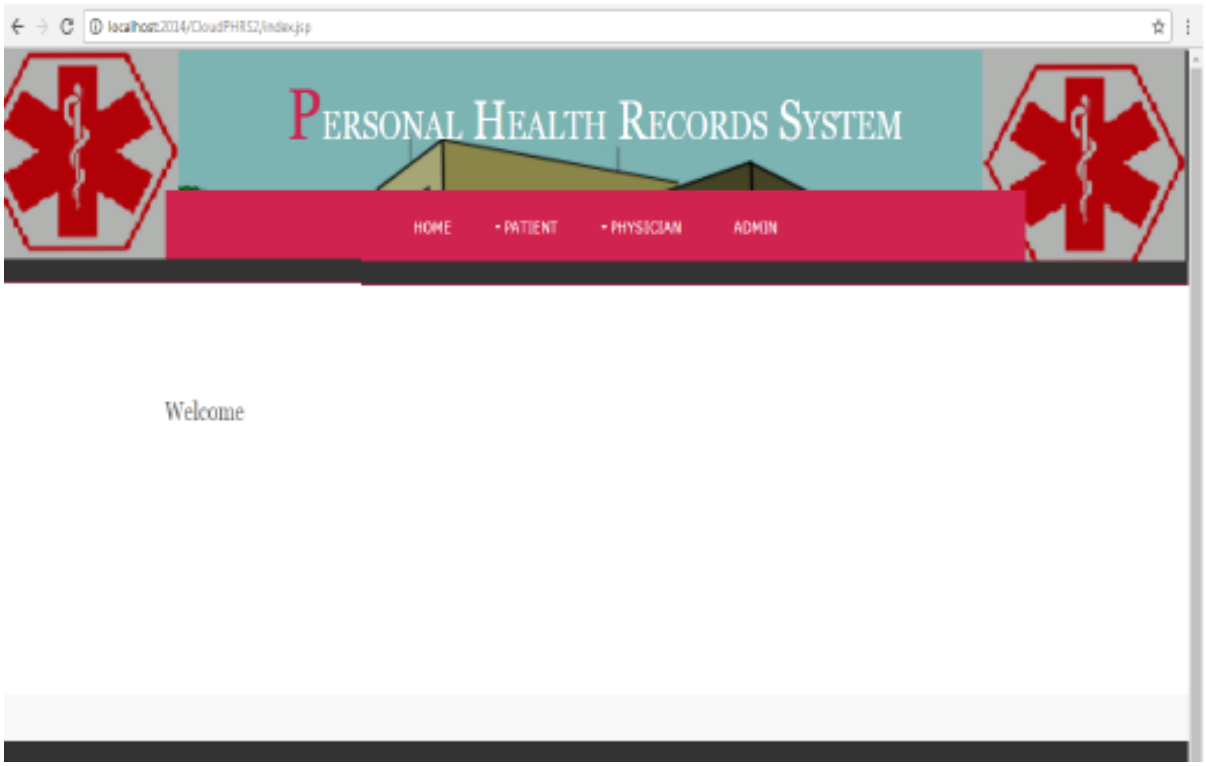

Figure 3: Home page of the proposed System

VII. CONCLUSION

In this project, the security and privacy concerns were addressed for cloud-based PHR system by integrating advanced cryptographic techniques, such as ECC, into PHR system. It was demonstrated that, by using appropriate cryptographic techniques, patients can protect their valuable healthcare information against a partially trustworthy server. To rapidly and securely transmit the health information in a wireless network, the electronic health information which utilizes the ECC security scheme to effectively encrypt the personal health records, is proposed.

VIII. FUTURE WORK

This study shows that the personal health records system is secure, scalable and efficient. The stem is basic but effective; there is room to improve the performance of the system by modifying the algorithm applied. Now that the developed system can secure the patient's medical records, also aim is to improve the performance and as well as to add more features to the system.

Conflict of Interest: The authors declare that they have no conflict of interest.

Ethical Statement: The authors declare that they have followed ethical responsibilities.

REFERENCES

[1] Christian Neuhaus, A. P. (n.d.). Survey on HealthcareIT Systems.
[2] Chang-Ji Wang, X.-L. X.-Y.-L. (2014). An Efficient Cloud-based Personal Health Records System Using Attribute-Based. IEEE, 978-1-4799-4171-1.

[3] G.Nikhita Reddy, G. R. (n.d.). Study of Cloud Computing in HealthCare Industry.
[4] Abdul Manan, I. (2014). Opportunities and Threats of cloud computing in Healthcare. International Journal of Computer Applications, 0975-887.
[5] Aruna Devi.S, M. (2014). Enhancing Security features in Cloud Computing for Healthcare using Cipher and intercloud. International Journal of Research in Engineering and Technology,200-203.
[6] G. Rathi, A. M. (2015). Healthcare Data Security in Cloud Computing. International Journal of Innovative Research in Computer and Communication Engineering, 1807-1815.
[7] Li, M.; Yu, S.; Ren, K.; Lou, W. Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings. In Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010), Singapore, 7–9 September 2010; pp. 89–106.

