Augmented Sh (Smarter Healthcare) Big Data Analytics With "Outsmart-Fgac Cloud Framework"

[1]Jayabharathi Gaddale
[1]Assistant Professor
[1]Department of Computer Science and Engineering
[1]KG Reddy College of Engineering and Technology, Moinabad, Hyderabad, India

Abstract: Nowadays the field of Big Data plays a vital role in various spheres. Big data is a term for massive data sets having a huge volume of data from different organizations, enterprises, and other businesses; healthcare data is continued data which has more varied and complex structure with the difficulties of data privacy, security, transformation, storing, analyzing, knowledge extraction, and visualization. In this paper our proposed work focuses on big data analytics to evaluate the quality of the research evidence on the smarter healthcare system using an augmented big data analytics with Outsmart-FGAC Cloud framework, which addresses the challenges with smart health care system and proves that how such information impacts the quality of attention on the smarter health care system.

Keywords: **Big Data Analytics, Smarter healthcare, Outsmart FGAC Cloud Framework, Cloud Computing.**

I.INTRODUCTION

Now days, Healthcare Information Technology (HIT) has capability to electronically store, maintain, and move data across the world in seconds of time and has ability to maintain healthcare with lot of increasing productivity and quality of services. Health information needs to be accessible and available to everyone involved in the delivery of patient healthcare from the researchers attempting to find causes, treatments, and cures for diseases to the patients themselves. The revolution in healthcare data size is another problem in today's Healthcare Information Systems (HISs) [1]. This revolution is not just about the massive size of healthcare data, but we also witness an exponential increase in the speed in which this data is generated and a complex varieties of data type (i.e., structured, semi structured, unstructured). The Development of new technologies such as capturing devices, sensors, and mobile applications is a major source of healthcare data [2]. Additional sources are added every day; patient social network communications in digital forms are increasing, collection of genomic information became cheaper and more medical knowledge/discoveries are being accumulated. Such big healthcare data is difficult to process or analyze using common database management tools. Obviously, capturing, storing, searching, and analyzing healthcare big data to find useful insights will improve the outcomes of the healthcare systems through smarter decisions and will lower healthcare cost as well, however, it requires efficient analytical algorithms and powerful computing environments.

Finally, the increased reliance on networked healthcare data brings new challenges to securing medical records in EHR systems. Authenticating individuals and authorizing global secure access to patients' records are vital security requirements. Physical face-to-face methods of identifying and authenticating patients and providers no longer apply; methods of electronic identification and authentication are required. Moreover, electronic records are susceptible to inappropriate access, compromised data integrity, or widespread unauthorized distribution. New security measures are needed to secure patients' records on HISs.

In this paper we introduce a framework for secure HISs based on big data analytics in mobile cloud computing environments. This framework provides a high level of integration, interoperability, and sharing of EHRs among HPs, patients, and practitioners. It integrates distinct EMRs of a patient from different HPs distracted among different cities, states, and regions and stores them in the Cloud data storage areas. Mobile Cloud computing technology provides a fast Internet access and provision of EHRs from anywhere and at any time with high availability [3]. Due to the massive size of healthcare data, the exponential increase in the speed in which this data is generated and the complexity of healthcare data type, the proposed framework employs big data analytics to find useful insights that help practitioners take critical decisions in the right time. Our proposed framework applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of medical data.

II. EXISTING SYSTEM

Improving healthcare services and reducing medical cost are the ultimate goals of nations worldwide. However, the revolutions of healthcare data size remains an obstacle that hinder achieve this goal. In 2012, worldwide digital healthcare data was estimated to be equal to 500 petabytes and is expected to reach 25,000 petabytes in 2020. Obviously, capturing, storing, searching, sharing and analyzing such big data to find useful insights will improve the outcomes of the healthcare systems through smarter decisions and will lower healthcare cost as well, however, traditional database management tools are no longer suitable to process these data[4]. New efficient algorithms are required to accomplish this task.

Big data analytics is motivated in healthcare through the following aspects:

- Healthcare data is now growing very rapidly in terms of size, complexity, and speed of generation and traditional database and data mining techniques are no longer efficient in storing, processing and analyzing these data. New innovative tools are needed in order to handle these data within a tolerable elapsed time.
- The patient's behavioral data is captured through several sensors; patients' various social interactions and communications.

- The standard medical practice is now moving from relatively ad-hoc and subjective decision making to evidence-based healthcare.
- Inferring knowledge from complex heterogeneous patient sources and leveraging the patient/data correlations in longitudinal records.
- Understanding unstructured clinical notes in the right context.
- Efficiently handling large volumes of medical imaging data and extracting potentially useful information and biomarkers.
- Analyzing genomic data is a computationally intensive task and combining with standard clinical data adds additional layers of complexity.

Security issues

In cloud-based HIS, security should be the top priority from day one. Patients' data should be protected with comprehensive physical security, data encryption, user authentication, and application security as well as the latest standard-setting security practices and certifications, and secure point-to-point data replication for data backup. These security issues have been extensively investigated for cloud computing in general. A major challenge to healthcare cloud is the security threats including tampering or leakage of sensitive patient's data on the cloud, loss of privacy of patient's information, and the unauthorized use of this information.

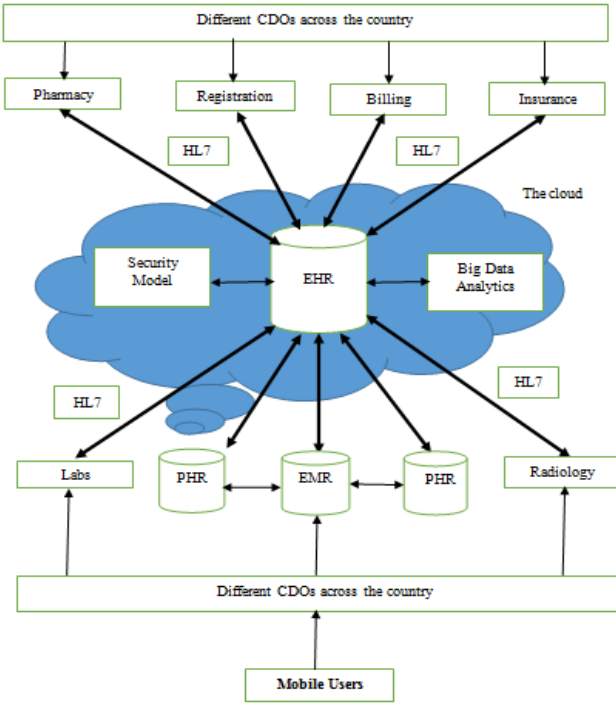

Fig. 1: A Framework for EHR based on mobile cloud computing and big data analytics

III.RELATED WORK

Smarter healthcare system

In recent years, mobile devices have started becoming abundant in many healthcare applications. The reason for the increasing usage of mobile computing is its ability to provide a tool to the user when and where it is needed regardless of user movement, hence, supporting location independence. However, it suffers some inherent problems such as limited scalability of users and devices, limited availability of software applications, resources scarceness in embedded gadgets, frequent disconnection and finite energy of mobile devices.

In healthcare sector, the effect of these limitations is magnified due to the massive size, excessive complexity, and rapid generation of healthcare data. As a result, a wide range of healthcare applications are difficult to run in mobile devices such as radiology processing and recognition, patients' social networking data management, genomic information and sensor data applications. In addition, progress in interoperation and sharing data among different EMR systems has been extremely slow due to the high cost and poor usability. What is needed is an environment that is capable of capturing, storing, searching, sharing and analyzing healthcare big data efficiently to provide right intervention to the right patient at the right time.

Cloud computing provides an attractive IT platform to cut down the cost of HER systems in terms of both ownership and IT maintenance burdens for many medical practices. Cloud environment can host EHRs and allows sharing, interoperability, high availability, and fast accessibility of healthcare data [6]. Cloud Computing (CC) platforms possess the ability to overcome the discrepancies of mobile computing with their scalable, highly available and resource pooling computing resources. The main idea behind CC is to offload data and computation to a remote resource provider (i.e., the Internet) which offers broad network access. The concept of offloading data and computations in the Cloud , is used to address the inherent problems in mobile computing by using resource providers (i.e., cloud resources) other than the embedded devices themselves to host the execution of user applications and store users' data.

The problems are addressed as follows:

1) By exploiting the computing and storage capabilities (resource pooling) of the cloud, mobile intensive applications can be executed on low resource and limited energy mobile devices

2) The broad network access of the cloud overcomes the limited availability and frequent disconnection problems since cloud resources are available in anywhere and at any time

3) The infrastructure of cloud computing is very scalable, cloud providers can add new nodes and servers to cloud with minor modifications to cloud infrastructure, therefore; more services can be added to the cloud, this allows more mobile users to be served and more portable devices to be connected.

Mobile cloud computing technology will contribute to healthcare sectors in the following ways:

Integrating healthcare data dispersed among different healthcare organizations and social media.

- Providing a shared pool of computing resources that is capable of storing and analyzing healthcare big data efficiently to take smarter decisions at the right time.
- Providing dynamic provision of reconfigurable computing resources which can be scaled up and down upon user demand. This will help reduce the cost of cloud-based healthcare systems.
- Improving user and device scalability and data availability and accessibility in healthcare systems.

Healthcare cloud can provide two deployment Models. These models describe the level of data sharing among different CDOs, patients, and practitioners when using the cloud.

These models are:

- Private healthcare cloud: The cloud infrastructure is owned solely by a CDO. It may be managed by the CDO or a CSP and may exist on or off premise. The CSP provides the same capability in terms of security and privacy protection as those in the EMR system running by a CDO.
- Community healthcare cloud: The cloud infrastructure is shared by several CDOs and supports a specific community that has shared concerns (e.g., mission, security requirements, and policy). It is managed by a CSP or by the CDOs and may exist on or off premise.

Healthcare services provided by healthcare clouds are classified as follows:

Software as a Service (SaaS): Healthcare applications, such as EHRs, are hosted as a service and provided to practitioners, healthcare providers, and patients across the Internet, with no need to install and run on their own computer. Hosted applications can be accessed through web browsers from various client devices such as laptops, PDAs and cell phones. Multiple users can share the applications and avoid the trouble associated with software maintenance, upgrading and the need for additional licenses.

Platform as a Service (PaaS): PaaS is a development platform that allows healthcare providers to not only deploy but also design, model, develop and test healthcare applications directly on the Cloud. It supports work in groups on collaborative healthcare projects where project team members are geographically distributed. This requires PaaS to provide development infrastructure including tools and programming languages.

Infrastructure as a Service (IaaS): healthcare providers can directly use independent virtual machines that isolate the underlying physical hardware of the cloud from them. They can dynamically provision/release virtual computing resources based on their increasing/decreasing resource demand.

IV. PROPOSED SYSTEM

However, in the new solution pattern, an advanced version of ABE called multi-authority ABE (MA-ABE) is used. In this encryption scheme, many attribute authorities operate simultaneously, each handing out secret keys for a different set of attributes.

Advantages

- ✓ It Avoids Key Escrow Problem.
- ✓ Maintain Better Security And Privacy.
- ✓ Complexity Of Key Management Greatly Reduced.
- ✓ Support Dynamic Policy Changes, Enforced Write Access Control.
- ✓ More Expressive File Access.
- ✓ Reduced Storage and Communication Cost.
- ✓ Enhances the System Scalability.

Fine Grained Data Access Control Framework

Cloud Authorization Framework: Our cloud authorization model is composed of the following parties: the owner organization that owns data and governs cloud infrastructure, different programmers inside the owner organization, who access cloud resources for different purposes and develop applications using cloud resources, and external clients who use the developed cloud applications as services [8]. Cloud applications have different components running on the end-user device or the company-managed cloud spaces, with the capability of migrating between them. Thus, an authorization framework is required to regulate and manage component migration and resource usage for different types of users and applications. The required authorization policy regulating access to different resources by different users must be defined at a higher level by the organization that owns both data and cloud resources. However, individual applications can further tighten these organization-wide accesses by defining their application specific policy. The framework currently supports both hard organization-wide and soft application-specific policies.

The authorization framework supports all these actions. Access control decisions are made based on the attributes of the requester, the resource, and the requested action using the predefined policy rules. The framework combines the advantages of attribute-based authorization system, actor programming paradigm, and elastic application development to support modern mobile-cloud applications. Current implementation uses the Akka programming language and regulates interaction between different application components distributed between end-user device and cloud spaces in addition to dynamic migration of components according to predefined organization wide regulations or end-user device limitations.

1. ***Revocable ABE***

   It is a well-known challenging problem to revoke users/attributes efficiently and on-demand in ABE. Traditionally this is often done by the authority broadcasting periodic key updates to unrevoked users frequently, which does not achieve complete backward/forward security and is less efficient.

2. ***Enhancing MA-ABE for user revocation***
   The original CC MA-ABE scheme does not enable efficient and on-demand user revocation. To achieve this for MA-ABE, it combines ideas from YWRL's revocable ABE and propose an enhanced MA-ABE scheme.
3. ***Enforce Write Access Control***
   If there is no restriction on write access, anyone may write to someone's PHR using only public keys, which is undesirable. By granting write access, it means a data contributor should obtain proper authorization from the organization she is in (and/or from the targeting owner), which shall be able to be verified by the server who grants/rejects write access.
4. ***ABE for Fine-grained Data Access Control***
   ABE to realize fine-grained access control for outsourced data especially; there has been an increasing interest in applying ABE to secure electronic healthcare records. An attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of unrevoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE)[7] to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline.
5. ***System Setup and Key Distribution***
   The system first defines a common universe of data attributes shared by every PSD, such as "basic profile", "medical history", "allergies", and "prescriptions". An emergency attribute is also defined for break-glass access. Each PHR owner's client application generates its corresponding public/master keys.

The public keys can be published via user's profile in an online healthcare social-network (HSN). There are two ways for distributing secret keys. First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in GoogleDoc. Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, and the owner will grant her a subset of requested data types.

6. ***PHR Encryption and Access***
   The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PHR files, excluding the server. For improving efficiency, the data attributes will include all the intermediate file types from a leaf node to the root. For example, in an "allergy" file's attributes are {PHR, medical history, allergy}. The data readers download PHR files from the server, and they can decrypt the files only if they have suitable attribute based keys. The data contributors will be granted write access to someone's PHR, if they present proper write keys.
7. ***User Revocation***
   Here it considers revocation of a data reader or her attributes/access privileges. There are several possible cases revocation of one or more role attributes of a public domain user, revocation of a public domain user which is equivalent to revoking that entire user's attributes. These operations are done by the AA that the user belongs to, where the actual computations can be delegated to the server to improve efficiency. Revocation of a personal domain user's access privileges. These can be initiated through the PHR owner's client application in a similar way.
8. ***Policy Updates***
   A PHR owner can update her sharing policy for an existing PHR document by updating the attributes (or access policy) in the cipher text. The supported operations include add/delete/modify, which can be done by the server on behalf of the user.
9. **Break-glass**
   When an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In this framework, each owner's PHR's access right is also delegated to an emergency department ED. To prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

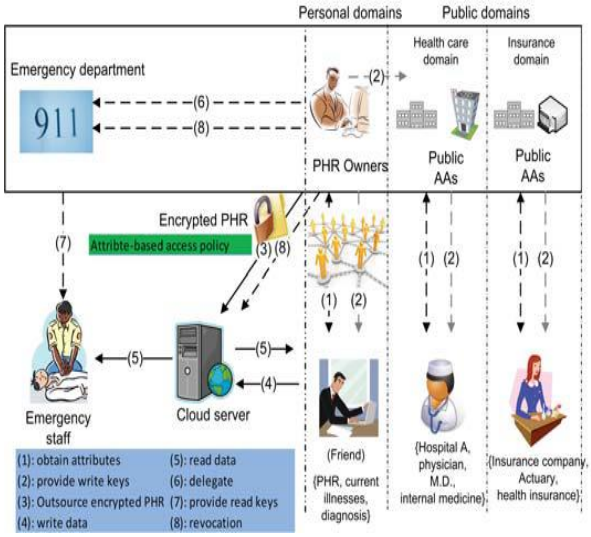

Fig. 2: The proposed framework for patient-centric, secure and scalable PHR sharing on semi trusted storage under multi owner settings

V. CONCLUSION AND FUTURE WORK

This paper proposes a framework for secure Health Information Systems (HISs) based on big data analytics in mobile cloud computing environment. The framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers, patients and practitioners. The cloud permits a fast Internet access, sharing, and provision of EHRs by authenticated users. Big data analytics helps analyze patient data to provide right intervention to the right patient at the right time. The proposed framework applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of medical data. The ultimate goal of the proposed framework is to introduce a new generation of HISs that are able to provide healthcare services of high quality and low cost to the patients using this combination of big data analytics, cloud computing and mobile computing technologies. In the future we plan to design and implement HIS based on the proposed framework.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'lICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89- 106, Sept. 2010.

[2] H. Lo¨ hr, A.-R.Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc.First ACM Int'l Health Informatics Symp.(IHI '10),pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems(ICDCS '11), June 2011.

[4] "The Health Insurance Portability and Accountability Act, "http://www.cms.hhs.gov/HIPAAGenInfo/01_Overvi w.asp,2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't ApplytoThem,"http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] H. Takabi, J. B. Joshi, and G.-J. Ahn. Secure cloud: Towards a comprehensive security framework for cloud computing environments. In *Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual*, pages 393–398. IEEE, 2010.

[7] G. Wang, Q. Liu, and J. Wu. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 735–737. ACM, 2010.

[8] S. Yu, C. Wang, K. Ren, and W. Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9. IEEE, 2010.