Access to Health Data from Mobile Devices, Assisted by the Cloud

With Privacy, Auditability and Customization Capabilities

Shiny Dhar, ShivalikaSuman, RoshelBritto, Sneha
ISE
JSSATE
Bangalore, India

***Abstract*—Privacy issues are increasingly becoming a cause of headaches for cloud users. Increasing use of cloud service models and e-healthcare systems has helped us to propose a private healthcare system with the health of a private cloud. Our system offers features of a smart key management system, privacy preservation of health data and retrieval with retrieval during emergencies and auditability. Specifically, we integrate key management from pseudorandom number generation for unlink ability, secure indexing method by preserving keyword search that hides access and search patterns and integrates the concept of attribute based patterns based on redundancy with attribute based encryption and threshold signing for role based access to prevent potential misbehavior in both normal and emergency cases. Also the user interface is customizable as the user wishes.**

***Index Terms*—Access control, e-Health, privacy, cloud computing, mobile access, customization**

I. INTRODUCTION

Cloud usage has increased rapidly since its inception. Retrieving, updating, viewing and accessing health data has led to a better and easier lifestyle. Services offered by this groundbreaking technology are mostly in the form of providing the electronic medical record (EMR) or electronic health record (EHR) as a service. There are multiple advantages to using cloud based services for implementing and deploying healthcare applications. For e.g.,we could easily and remotely access health data during emergencies and otherwise, without maintaining any hardware related to storage. But people completely lose control over their data once it has been uploaded to the cyberspace. A very recent security breach has been the one the second largest health insurance company in USA,the Anthem Inc.[1], on February 2nd this year. A mass of 80 million customers faced the risk of their health data being stolen including the CEO of the company as reported by a popular daily. Also if leaked it might be difficult to get health insurance or even a job. Thus there is a dire need in developing systems that are secure with privacy protection and auditability properties when using the cloud.

In order to ensure that, we propose a system that uses the SaaS approach shown in Figure 1. The users log in to the private cloud that provides the SaaS services and the data is then encrypted and stored on the public cloud. This approach leaves the users with lightweight tasks.

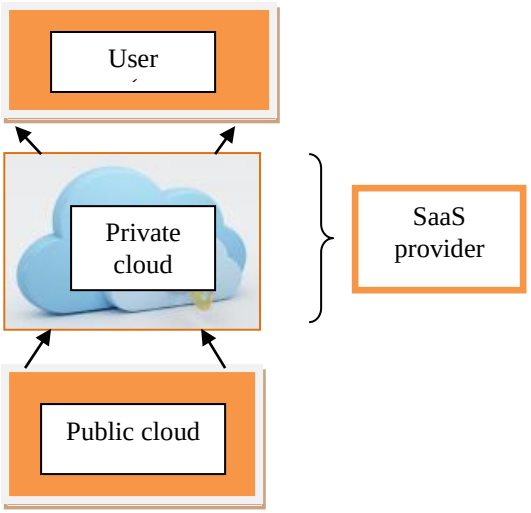

Fig. 1. SaaS model implemented

II. ALGORITHMS USED AND RELATED STUDY

A. *Related study:MIPA*

Medical Information Privacy Assurance(MIPA)[] was one of the early projects that studied the development of systems that enforced security; so that individuals could protect their personal data. It was one of the first projects that talked about the devastating effect of breaches in e-health data and also the challenges in designing these systems so that they could be made more secure.

Sun *et al* [] had published a paper on privacy preservation of heath data storage that is of most relevance to this paper along with SSE schemes. In the paper, they suggested the use of encryption by the users of their data and storing it on a third party server.

Tan *et al* [] proposed a role based approach to allowing access to health data. Although the implementation lacked in major areas, access based on roles is used here too.

B. Searchable Symmetric Encryption

SSE is used to search over encrypted documents. At a high level, the algorithms in order to do that are taken from Curtmola*et al.*[2] They are briefly described below as:-

Keygen(1k) is a probabilistic key generation algorithm that is run by the user to setup the scheme. It takes a security parameter k, and returns a secret key K such that the length of K is polynomially bounded in k.

BuildIndex(K, D) is a (possibly probabilistic) algorithm run by the user to generate indexes. It takes a secret key K and a polynomially bounded in k document collection D as inputs, and returns an index I such that the length of I is polynomially bounded in k.

Trapdoor(K, w) is run by the user to generate a trapdoor for a given word. It takes a secret key K and a word as inputs, and returns a trapdoor T_w.

Search(I, Tw) is run by the server S in order to search for the documents in D that contain word w. It takes an index I for a collection D and a trapdoor Tw for word w as inputs, and returns D(w), the set of identifiers of documents containing w.

The algorithms ensure safe and secure search and takes the party that searches as a curious yet honest third party server. In Curtmola's version, each document is marked by an identifier and relates to a node. These documents are spread randomly in multiple cloud servers (might be at geographically dispersed locations). They are tracked and data is accessed with the help of an array A and a look up table T. The trapdoor T_w is used to retrieve documents from the remote server into the lookup table, thereby allowing access.

C. Identity Based Encryption

Founded by Bonch and Franklin[1], identity-based systems proposed any 3rd party to generate a public key from a known identity.
For example,the string "D/O of SC Dhar" for Shiny.
Distributing keys beforehand isn't required by this method.
It is an application of the pairing-based cryptography.

D. Attribute Based Encryption

Identity-based cryptography and in particular identity-based encryption (IBE) . ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes .The key issue is, that one can only be able to decrypt a cipher text if the he or she holds a key for those "matching attributes". Noteworthy here is that the keys are always issued by some trusted party.

III. EXISTING AND PROPOSED SYSTEM

A. Existing System

Cloud based applications today are not secure enough because of the following reasons:-

- Privacy issues aren't addressed appropriately.
- Storage pattern is weak as it doesn't hide search and access patterns.
- Shortage of protocols and systems to safeguard personal digital information.

The proposed system has the following advantages:-

- Inspired by cloud based outsourcing paradigm.
- Based on SaaS model of cloud computing.
- It provides higher security as it has cryptographic mechanisms.
- Lightweight tasks are left to users.

B. System model

The architecture of the proposed system is shown in Figure 2: Users collect their health data through the monitoring devices worn or carried, e.g., electrocardiogram sensors and health tracking patches. Emergency medical technician (EMT) is a physician who performs emergency treatment. By user and EMT, we refer to the person and the associated computing facilities.
The computing facilities are mainly mobile devices carried around such as smartphone, tablet, or personal digital assistant.
Each user is associated with one private cloud. Multiple private clouds are supported on the same physical server. Private clouds are always online and available to handle health data on This can be very desirable in situations like medicalemergencies.The private cloud will process the data to add security protection before it is stored on the public cloud. Public cloud is the cloud infrastructure owned by the cloud providers.

C. Threat model

The private cloud is fully trusted by the user to carry out health data-related computations. Public cloud is assumed to be honest-but-curious, in that they will not delete or modify users' health data, but will attempt to compromise their privacy. Public cloud is not authorized to access any of the health data.The EMT is granted access rights to the data only pertinent to the treatment, and only when emergencies take place. The EMT will also attempt to compromise data privacy by accessing thedata he/she is not authorized to.
Finally, outside attackers will maliciously drop users' packets, and access users' data though they are unauthorized to.Figure 3 shows the use cases for the system .

Fig. 2 Cloud-assisted mobile health network.

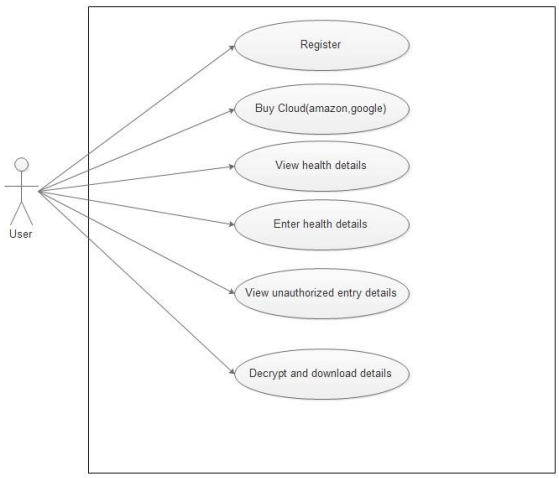

Fig. 2 Use case model for the diagram

D. *Security Requirements*

In this paper, we strive to meet the following main security requirements for practical privacy-preserving mobile healthcare systems.

1) *Storage Privacy:* Storage on the public cloud is subject to five privacy requirements.

a) *Data confidentiality:* unauthorized parties (e.g., public cloud and outside attackers) should not learn the content of the stored data.

b) *Anonymity:* no particular user can be associated with the storage and retrieval process, i.e., these processes should be anonymous.

c) *Unlinkability:* unauthorized parties should not be able to link multiple data files to profile a user. It indicates that the file identifiers should appear random and leak no useful information.

d) *Keyword privacy:* the keyword used for search should remain confidential because it may contain sensitive information, which will prevent the public cloud from searching for the desired data files.

e) *Search pattern privacy:* whether the searches were for the same keyword or not, and the access pattern, i.e., the set of documents that contain a keyword should not be revealed. This requirement is the most challenging and none of the existing efficient SSE [14]–[17] can satisfy it. It represents stronger privacy which is particularly needed for highly sensitive applications like health data networks.

2) *Auditability:* In emergency data access, the users may be physically unable to grant data access or without the perfect knowledge to decide if the data requester is a legitimate EMT.

IV. IMPLEMENTATION

Our cloud-assisted privacy-preserving mobile healthcare system consists of two components:

- searchable encryption and
- auditable access control. Upon receiving the health data from

users, the private cloud processes and stores it on public cloud such that storage privacy and efficient retrieval can be guaranteed. Next, the private cloud engages in the accessing of data access and auditability scheme with users so that it can later act on the users' behalf to exercise access control and auditing on authorized parties.

A. *Privacy and Retrieval without links*

The first component is storage privacy for the health data. Our storage mechanism relies on secure index or SSE, so that the user can encrypt the data with additional data structures.In our environment, the private cloud takes the role of user, and the public cloud is the storage server in SSE.Our proposed pattern hiding scheme justslightly increases the computation and storage costs at the public cloud compared to the most efficient construction.

*1) Constructing the Secure Index:*The private cloud prepares data received from the user for privacy-preserving storage by constructing the index.

2) Encrypting the Data Files

3)Hiding the Patterns

4) Retrieving the Data Files

Figure 4 shows the activity diagram of implementation.

B. *Access to data and Auditing Capacity with a customizable UI*

The second component is the data access during emergencies where the EMT requests data through the private cloud. The proposed approach is for the general data access, although we focus on the emergency access since it is more challenging.We propose to combine signaturewith ABE-based access control.A(k, n) threshold signature thatguarantees that a valid signature on a messagecan be generated as long as there are k valid signature shares. For instance, we can set n = 5

representing the privatecloud, the primary physician, the EMT, the specialists (e.g., pediatrician
and urologist), and the insurance provider.
User interface is made friendly according to the type and severity of the data stored.

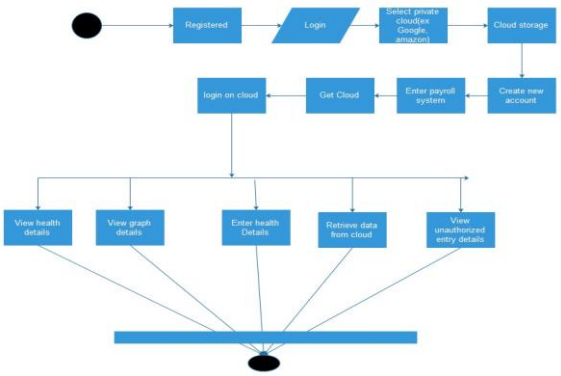

Fig 4. Activity diagram for proposed system

V. CONCLUSION

In this paper, we proposed to build privacy into mobile health systems with the help of the private cloud. We provided a solution for privacy-preserving data storage by integrating key management for unlinkability, a search and access pattern hiding scheme based on redundancy, and a secure indexing method for privacy-preserving keyword search. We also investigated techniques that provide access control (in both normal and emergency cases) and auditability of the authorized parties to prevent misbehavior, by combining ABE-controlled threshold signing with role-based encryption. As future work,

- we plan to devise mechanisms that can detect whether users'health data have been illegally distributed,
- and identify possiblesource(s) of leakage (i.e., the authorized party that did it).

VI. REFERENCES

[1] C. Wang, K. Ren, S. Yu, and K. Urs, "Achieving usable and privacy assured similarity search over outsourced cloud data," in *Proc. IEEE Conf. Comput. Commun.*, Mar. 2012, pp. 451–459.
[2] N. Cao, Z. Yang, C.Wang, K. Ren, andW. Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst.*, Jun. 2011, pp. 393–402.
[3] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on PHI in ehealthcare systems," *Adv. Health Inform. Conf.*, pp. 1–5, Apr. 2010.
[4] M. Katzarova and A. Simpson, "Delegation in a distributed healthcare context: A survey of current approaches," in *Proc. 9th Int. Conf. Inform.*
[5] U.S. Department of Health & Human Service, "Breaches Affecting 500 orMore Individuals," (2001). [Online].Available:tp://www.hhs.gov/ocr/ privacy/hipaa/administrative/breachnotificationr ule/breachtool.html
[6] www.usatoday.com