ACCESSING HEALTH RELATED DATA USING CLOUD VIA AUDITABILITY

[#1]Mr.Amol N. Dumbare, [#2]Mr. Nilesh B. Korade

[1]amol.dumbare@pccoer.in
[2]nilesh.korade@pccoer.in

[#12]Computer Engineering Department,

PCET's Pimpri Chinchwad College of Engineering and Research,
Ravet, Pune, Maharshatra.

ABSTRACT

Motivated by the privacy issues, curbing the adoption of electronic healthcare systems and the wild success of cloud service models. We introduce the private cloud which can be considered as a service offered to mobile users. With the help of the private cloud, we propose to build privacy into mobile healthcare systems. The features that our system offers including privacy-preserving data storage and retrieval, efficient key management, especially for retrieval at emergencies, and audit ability for misusing health data. For privacy preserving keyword search, we provide a secure indexing method which hides both search and access patterns based on redundancy, for providing role-based access control with audit ability to prevent potential misbehavior, in both normal and emergency cases, it integrate the concept of attribute based encryption with threshold signing.

Keywords: **Auditability, access control, eHealth, privacy.**

ARTICLE INFO

Article History

Received: 6th June 2017

Received in revised form :

6th June 2017

Accepted: 8th June 2017

Published online :

9th June 2017

I. INTRODUCTION

A. Problem Statement

All, users or data owners are not in a good position to determine who needs access to which data files. This is one of the most important features of health data access which requires flexibility and professional judgment. In the proposed mobile health networks the authenticity of the attributes cannot be verified which is a very practical problem and highly challenging. Where a set of attributes is defined for each general role for example primary physician, EMT, and insurance provider that will access the data.

B. Goals and Objective

Input Design for converting a user-oriented description of the input into a computer-based system is important to avoid errors in the data input process and for getting correct information from the computerized system it shows the correct direction to the management. Making data entry easier and to be free from errors is the goal of designing input. It's designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities. When the data is entered it will check for its validity. Appropriate messages are provided as when needed so that the user will not be in maize of instant.

C. Basic Idea

Today's people are getting dependent more on web technologies like internet. Many user-centered platforms are now available for information sharing and user interaction, such as Epinion, Amazon, Facebook and Twitter. Nowadays when people are interested in a product or a service, they not only look for official information from pro service providers, but from experienced and practical opinions of the customers or users points of view are also efficacious. Recent state-of-the-art approaches such as frequency-based, relation-based, supervised learning or topic modeling showed that favorable results could be obtained. How to effectively analyze and exploit such immense online information source is a challenge. Fast access to medicinal review and prescribed health data enables better healthcare service provisioning, improves quality of life, and helps saving life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in our daily life.

II. LITERATURE SURVEY

A. Yue Tong, Jinyuan Sun, Sherman S. M. Chow, Pan Li, "Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability"

We studied the proposed mobile healthcare systems to build privacy with the help of the private cloud. We also studied the features offered by system including key management, privacy-preserving data storage, and retrieval, etc.

B. P. Ray and J. Wimalasiri, " The need for technical solutions for maintaining the privacy of EHR"

Include EPR (Electronic Patient record) HER (Electronic Health record) and EMR (Electronic medical Record). This record is used by many health providers it is essential to provide privacy to the system.

C. Charalampos Doukas, Thomas Pliakas, Ilias Maglogiannis , "Mobile healthcare information management utilizing Cloud Computing and Android OS"

We studied the implemented mobile system which enables electronic healthcare data storage, update and retrieval using Cloud Computing.

III. ARCHITECTURE

Fig 1. Architectural Block Diagram

We refer to the person and the associated computing facilities which are mobile devices carried around such as smart phone, tablet or PDA. User collects their health data through the monitoring devices. Each user is associated with one private cloud supported on the same physical server. It is always online and available to handle health data on behalf of the users and fully trusted by the user to carry out the heath data-related computations. The public cloud is assumed to be honest but curious, they will not modify users health data, but will attempt to compromise their privacy. It is not authorized to access any of the health data. There isa secure channel between the user and his private cloud for example Secure home Wi-Fi network to negotiate a long term shared key. Access rights to the data are granted by EMT only pertinent to the treatment and only when emergency takes place. It will also attend to compromise data privacy by accessing the data he is not authorized to. Through internet backbone user will send health data over insecure network to the private cloud. The proposed system do not focus on the location privacy of mobile users which can be leaked when sending health data to the private cloud. It also assumes outside attackers will maliciously drop users' packets, and access user data through they are unauthorized.

IV. MATHEMATICAL FORMULATION

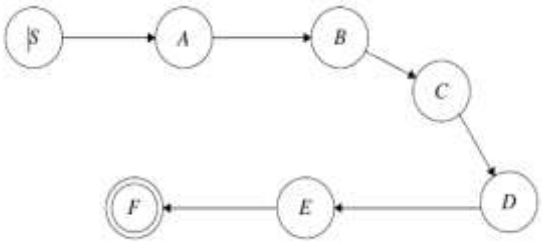

Fig 2. Mathematical Formulation

S=Start State
A=Medical Information Privacy Assurance(MIPA)
B=Searchable Symmetric Encryption
C=Identity-Based Encryption
D=Attribute-Based Encryption
E=Security Requirements
F=Final State
Success Conditions: Privacy of data is maintained
Failure Conditions: Data is leaked due to lack of privacy

V. ABE-BASED ACCESS CONTROL

We propose to combine threshold signature with ABE-based access control. Let A(k, n) be a threshold signature provides guarantees that a valid signature on a message can be generated as long as there are k valid signature shares.
We can set n =5 representing the private cloud, the primary physician, the specialists (e.g., pediatrician and urologist), the EMT, and the insurance provider. Let k =2 such that any not fully trusted party must perform the threshold signing with either fully trusted party. The private cloud and primary physician are fully trusted by the user. The EMT better performs the signing with the private cloud because the primary physician may not be available online at all times. On the other hand, a pediatrician better performs the signing with the primary physician since users normally rely on their primary physicians for referral to a specialist.

In proposed design, users do not encrypt their health data using ABE. Instead, users use ABE to encrypt the secret shares so that only authorized parties can decrypt them and generate valid signatures.

The user can check the request and the validity of the threshold signature to audit the following at a later time: First the request was due to a true medical emergency, Second the EMT has requested data only pertinent to the treatment, Third the EMT cannot deny the data request and access if either first or second is violated, and fourth the private cloud cannot falsely accuse the EMT if neither first nor second is violated. In doing so, users avoid the daunting task of determining who can access which data files. They only need to determine who can access their data and assign a secret share correspondingly. We also propose to leverage the existing healthcare system architecture to verify the authenticity of the attributes.

ABE-Controlled Threshold Signing: The user secret-shares a key to n participating parties.

1. For ABE-controlled thresh-old signing User defines some parameters. Let $H:\{0,1\}*\rightarrow G$ be a hash function. Let G_1be a bilinear group of prime

order p_1, g and g_1 be generators of G_1, and e:$G_1 \times G_1 \rightarrow G_2$ be a bilinear map.

2. User (k, n) – shares x such that any subset S of k or more can reconstruct x using the Lagrange interpolation : $x = \sum i \in s\ L_i\ x_i$, where L_i are the appropriate Lagrange coefficients for the set S, and x_i are the secret shares.

3. User ABE-encrypts the secret share x_d for EMT, de-noted by ABE (x_d), as: Define the universe of attributes U={1,2,...,u} and a hash function $h:\{0,1\}* \rightarrow G_2$.

4. The public parameters are $V_1 = g_1^{v1}$,...,$Vu=g_v^{u1}$,$Y=e(g1,g1)^z$, and the master secret key is (v_1,...,v_u ,z).

5. User generates the decryption key D for EMT using the ABE key generation algorithm and sends ($ABE(x_d)$,$IBE_{Role}(D)$) to the private cloud, using the general role Role =EMT as the public key.

6. When EMT requests medical data from the private cloud, EMT sends the attributes g , the attribute certificate $(g)_{sig}$, and REQ which contains the keyword for search and the time range of interest. The private cloud verifies using $(g)_{sig}$ and returns ($ABE(x_d)$,$IBE_{Role}(D)$) to EMT. EMT first decrypts for D using the private key corresponding to the role "EMT," and then decrypts for x_d using D.

7. Private cloud and EMT each generates partial threshold signatures $\sigma_i=(H(REQ))^{xi}$, and exchange σ_i and $y_i = g^{xi}$. They verify the partial signature from each other by checking if (g,y_i, $H(REQ),\sigma_i$)is a valid Diffie–Hellman tuple.

8. Private cloud and EMT generate the threshold signature $\sigma=\prod_i \in_s(\sigma_i^{Li})$ which can be verified by anyone by checking if (g, y, H(REQ),σ)is a valid Diffie–Hellman tuple. The private cloud stores σ_i from EMT, σ, REQ, and the date/time request is made.

VI. PERFORMANCE EVALUATION

A. Storage and Communication Efficiency

We investigate the capacity and correspondence productivity by taking a gander at the capacity and correspondence overheads amid information outsourcing and recovery. The overhead is characterized to be any data that fills the needs of administration, security, accounting, and so forth, yet the vital social insurance information or its encryption. For clarity, we decay the correspondence into two sections, i.e., correspondence between information requesters, for example, EMT, and the private cloud and that between the private cloud and the general population cloud. It merits saying that albeit, as should be obvious from the table, the example concealing obliges recovering repetitive records amid information recovery, which appears to essentially add to the overhead, it happens just between the private furthermore, open cloud where the wired inter cloud association is steady what's more, quick, making the expanded information exchanging time irrelevant. Then again, the private cloud sends just the asked record to EMT (potentially through remote channels, which are moderately less unsurprising and of lower limit). Along these lines, it does not influence the general execution all that much. From the investigation above, we realize that the stockpiling overhead is direct with the quantity of outsourced human services information documents, while the correspondence overhead can be considered as steady per information demand. The outcome shows that the proposed plan is effective and additionally adaptable.

B. Computation Efficiency

In this area, we break down the computational productivity of the proposed plans. In particular, we are occupied with whether our plans are proficient when cell phones are included, i.e., patients setting up the protection safeguarding stockpiling and EMTs getting to the restorative information in crises. We executed our plans utilizing Samsung Nexus S cell phones (1-GHz CortexA8, 512-MB RAM) and measured the runtime. For executions of IBE and ABE, we utilized the Java Paring-Based Cryptography Library and utilized a blending amicable sort A 160-bit elliptic bend bunch. We compress the most excessive continuous processing on EMT cell phones in Table1. The cell phone we utilized is not the most recent model. The runtime is required to enhance with more up to date furthermore, all the more intense models. For correlation, we likewise give in the table the runtime of the same execution on a portable PC (Intel Core i5, 4-GB RAM), which can likewise be viewed as a cell phone. Generally, for every entrance, it takes around 16 s to perform the obliged cryptographic processing utilizing the picked cell phone and around 0.6 s on the portable workstation, both of which are worthy for a productive recovery of electronic human services records.

Table 1. Runtime of cryptography Operation

Operations	Avg. Runtime on smartphone	Avg. Runtime on laptop
ABE Decryption	8283ms	420ms
IBE Decryption	3509ms	140ms
AES Encryption	2.80MB/Sec	224.90MB/Sec
AES Decryption	2.30MB/Sec	190.80MB/sec

VII. CONCLUSION

With the help of the private cloud we try to build privacy into mobile health systems. We provided a solution for privacy-preserving data storage by integrating a PRF(pseudo random function) based key management 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 audit ability 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 possible source(s) of leakage (i.e., the unauthorized party that did it).

ACKNOWLEDGEMENT

I would like to take this opportunity to thank our HOD Mr. Salunke M. B. for giving me all the help and guidance I

needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful. I am also grateful to Dr. Tiwari H. U. Principal, Pimpri Chinchwad College of Engineering and Research, Ravet for his indispensable support, suggestions. In the end our special thanks to team members for providing various resources such as laboratory with all needed software platforms, continuous Internet connection etc.

REFRENCES

[1] Yue Tong, Jinyuan Sun, Sherman S. M. Chow, Pan Li, "Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability", IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. 18, NO. 2, MARCH 2014.

[2] P. Ray and J.Wimalasiri, "The need for technical solutions for maintaining the privacy of EHR," in *Proc. IEEE 28th Annu. Int. Conf.*, New York City,NY, USA, Sep. 2006, pp. 4686–4689.

[3] Charalampos Doukas, Thomas Pliakas, Ilias Maglogiannis , "Mobile healthcare information management utilizing Cloud Computing and Android OS".

[4] U.S. Department of Health & Human Service, "Breaches Affecting 500 or More Individuals," (2001). [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/ administrative/breachnotificationr ule/breachtool.html

[5] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care," presented at the 14th Int. Workshop Database Expert Syst. Appl., Prague, Czech Republic, 2003.

[6] G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis, "Medical information privacy assurance: Cryptographic and system aspects," presented at the 3rd Conf. Security Commun. Netw., Amalfi, Italy, Sep. 2002.

[7] L. Zhang, G. J. Ahn, and B. T. Chu, "A role-based delegation framework for healthcare information systems," in *7th ACM Symp. Access Control Models Technol.*, Monterey, CA, USA, 2002, pp. 125–134.

