SEMINAR

CS 4098

By
Blesson Andrews Varghese
(B110087CS)

Dept Of Computer Science and Engineering
NIT Calicut

Sept 25, 2014

Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability

[Based on research paper by Yue Tong , Jinyuan Sun, Sherman S. M. Chow, and Pan Li]

Structure Of Presentation

- Introduction
- Security Requirements
- Need for Privacy
- Earlier works
- Limitations of existing System
- Proposed system, Architecture
- Proposed pattern hiding scheme
- Retrieving data files
- Storage and Communication efficiency
- Computation efficiency
- Advantage of proposed system
- Minimum hardware and software configuration
- Conclusion

Introduction

- This paper propose to *build privacy into mobile healthcare systems* with the help of the private cloud.
- Newly proposed system offers salient features including efficient key management and privacy. At the same time it preserves old data storage, and retrieval mechanisms
- This paper introduces integrate key management from mere *pseudorandom number generator* for unlink ability to a *secure indexing method* for privacy preserving keyword search.

Security Requirements

we strive to meet the following main security requirements for practical privacy preserving mobile healthcare systems.

- Storage Privacy: Storage on the public cloud is subject to five privacy requirements:
  - Data confidentiality: Unauthorized parties (outside attackers) should not learn the content of the stored data.
  - Anonymity: No particular user can be associated with a single storage and retrieval process.

Security Requirements

- Unlink ability: It indicates that the file identifiers should appear random and leak no useful information.
- 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.
- Search pattern privacy: The set of documents that contain a keyword, should not be revealed.

Security Requirements

- 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.

Need for privacy in mobile healthcare systems

- E-healthcare systems are increasingly becoming popular nowadays. A large amount of personal data for medical purpose are involved.
- We may completely lose control over our personal information once it enters into the cyberspace. According to US government website, around 8 million patient's health information was leaked in the past two years.
- One person's medical data may be used by

Need for privacy in mobile healthcare systems

several people in several ways for their advantage. For example

- An employer may decide not to hire someone with certain diseases.
- An insurance company may refuse to provide life insurance knowing the disease history of a patient

- Therefore we must keep our medical data private and access-limited

Earlier Works

- Some early works on privacy protection for e-health data concentrate mainly on
  - the framework design: demonstration of the significance of privacy for e-health systems
  - authentication based on existing wireless infrastructure
  - role-based approach for access restrictions, etc.

- Earlier, patients encrypt their own health data and store it on a third-party server

Earlier Works

MIPA

- Among the earliest efforts on e-health privacy, Medical Information Privacy Assurance (MIPA) pointed out the importance and unique challenges of medical information privacy. MIPA showed the devastating privacy breach facts that resulted from insufficient supporting technology.
- MIPA was one of the first few projects that sought to develop privacy technology and privacy-protecting infrastructures to

Earlier Works

facilitate the development of a health information system, in which individuals can actively protect their personal information..

SSE

- SSE allows data owners to store encrypted documents on remote server, which is modeled as honest-but-curious party, and simultaneously provides away to search over the encrypted documents.

Earlier Works

- It consisted of four functions: Key_Gen(s) Build_Idx(D,K),Trapdoor(K ,w) and Search(I,Tw):
- . Key_Gen(s) is used by the users to generate keys to initialize the scheme.
- Build_Idx(D,K) helped to build the indexes, denoted by I, for a collection of document D. It takes the secret key K and D and outputs I, through which document can be searchable while remaining encrypted.
- The function takes the secret key K and the keyword w and outputs the respective trapdoor Tw . A trapdoor Tw can also be interpreted

Earlier Works

proxy for w in order to hide the real meaning of w.

- Search(I,Tw) is executed by the remote server to search for documents containing the user defined keyword w. Due to the use of the trapdoor, the server is able to carry out the specific query without knowing the real keyword. It outputs the identifiers of files which contains keyword w

IBE

Earlier Works

- Identity-based systems(IBE) allow any party to generate a public key from a known identity value, for example, the string "alice@xyz.com" for Alice. A practical IBE scheme in the random oracle model was proposed by Bone h and Franklin .
- IBE makes it possible for any party to encrypt message with no prior distribution of keys between individuals.

Threshold Secret Sharing

Earlier Works

- It is a mechanism for sharing secret information among multiple entities so that the cryptographic power is distributed. Hence it avoids a single point of failure. For (k, n) threshold secret sharing, a piece of information I is divided into n pieces $I_1, I_2, I_3 . . ., I_n$, such that knowledge of any k or more of these I_i ($i \in [1, n]$) pieces can recover I, while knowledge of (k − 1) or fewer pieces keeps I completely undetermined

Earlier Works

- Shamir proposed such a scheme based on polynomial interpolation

ABE

- In Attribute-Based Encryption(ABE), data are encrypted by the owner using a set of attributes.

- The parties accessing the data are assigned access structures by the owner and can decrypt the data only if the access structures match the data attributes.

Limitations of Existing System

- Privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short.

- The storage privacy in the existing system is a weaker form of privacy because it does not hide search and access patterns.

- There is a shortage of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information.

Proposed System

- Any medical company’s total claims capture and control(TC3) which provides claim management solutions for healthcare payers (insurance companies, Municipalities)has been using Amazon’s EC2 cloud to process the data their clients send in (tens of millions of claims daily) which contain sensitive health information.
- Outsourcing the computation to the cloud saves TC3 from buying and maintaining servers, and allows TC3 to take advantage of Amazon’s expertise to process and analyze

Proposed System

data faster and more efficiently.

- The proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the cloud-based data/ computation outsourcing paradigm.
- We introduce the private cloud which can be considered as a service offered to mobile users. The proposed solutions are built on the service model shown in figure.

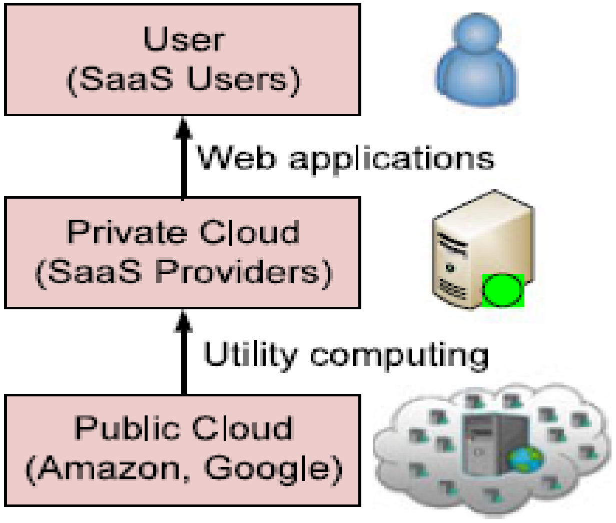
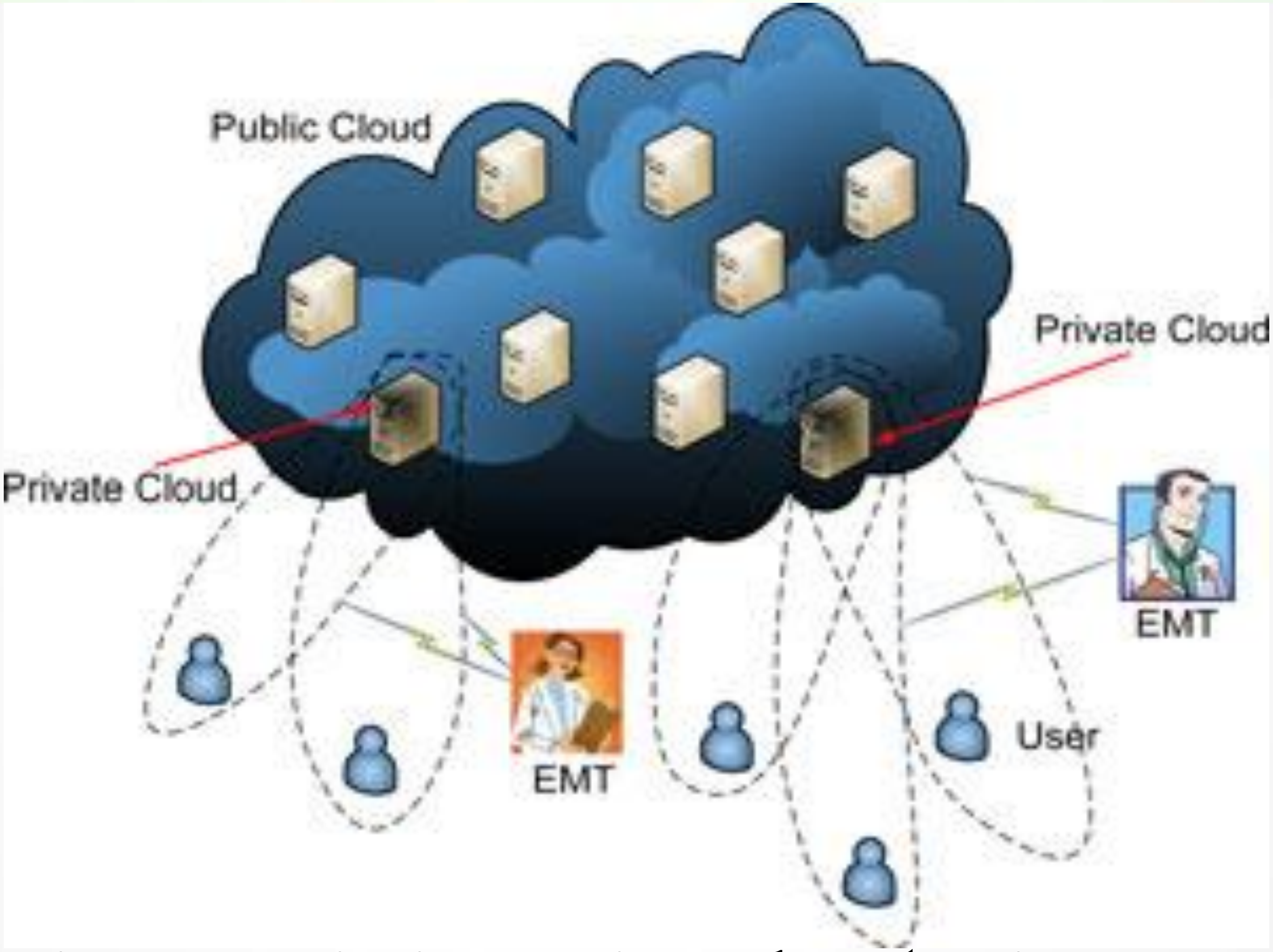


Fig. 1. SaaS service model.

Proposed System

- A software as a service(SaaS) provider provides private cloud services by using the infrastructure of the public cloud providers (e.g., Amazon).
- Mobile users outsource data processing tasks to the private cloud which stores the processed results on the public cloud.
- The cloud-assisted service model supports the implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks.

Architecture



- The main entities involved in proposed system are depicted in the above figure.

Architecture

- 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. Users collect their health data through the monitoring devices worn or carried.
- 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 behalf of the users.

Architecture

- The private cloud is fully trusted by the user to carry out health data-related computations. 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 such as Amazon and Google which offers massive storage and rich computational resource. 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

Architecture

their privacy. Public cloud is not authorized to access any of the health data.

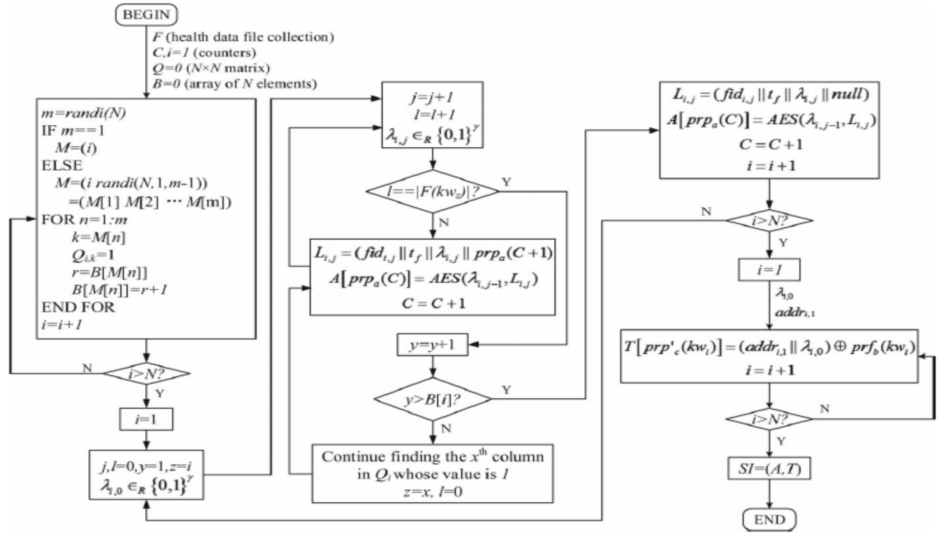
- There exists a secure channel between the user and his/her private cloud(e.g., secure home Wi-Fi network) to negotiate a long-term shared-key.
- The EMT is granted access rights to the data only pertinent to the treatment, and only when emergencies take place. The EMT will also attempt to compromise data privacy by accessing the data he/she is not authorized to. The EMT is assumed to be rational in

Architecture

the sense that he/she will not access the data beyond authorization if doing so is doomed to be caught.

- Later, user will send health data over insecure network to the private cloud residing via the Internet backbone.
- 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 users data though they are unauthorized to.

proposed pattern hiding scheme


BEGIN
F (health data file collection)
$C, i=1$ (counters)
$Q=0$ ($N \times N$ matrix)
$B=0$ (array of N elements)
$m=randi(N)$
IF $m==1$
$M=(i)$
ELSE
$M=(i\ randi(N,1,m-1))$
$=(M[1]\ M[2] \cdots M[m])$
FOR $n=1:m$
$k=M[n]$
$Q_{i,k}=1$
$r=B[M[n]]$
$B[M[n]]=r+1$
END FOR
$i=i+1$
N
$i>N?$
Y
$i=1$
$j,l=0, y=1, z=i$
$\lambda_{i,0} \in_R \{0,1\}^\gamma$
$j=j+1$
$l=l+1$
$\lambda_{i,j} \in_R \{0,1\}^\gamma$
$l==|F(kw_z)|?$
Y
N
$L_{i,j}=(fid_{i,j} \| t_f \| \lambda_{i,j} \| prp_a(C+1))$
$A[prp_a(C)]=AES(\lambda_{i,j-1}, L_{i,j})$
$C=C+1$
$y=y+1$
$y>B[i]?$
Y
N
Continue finding the x^{th} column in Q_i whose value is 1
$z=x, l=0$
$L_{i,j}=(fid_{i,j} \| t_f \| \lambda_{i,j} \| null)$
$A[prp_a(C)]=AES(\lambda_{i,j-1}, L_{i,j})$
$C=C+1$
$i=i+1$
N
$i>N?$
Y
$i=1$
$\lambda_{i,0}$
$addr_{i,1}$
$T[prp'_c(kw_i)]=(addr_{i,1} \| \lambda_{i,0}) \oplus prf_b(kw_i)$
$i=i+1$
$i>N?$
N
Y
$SI=(A,T)$
END

Pattern hiding secure index.

- Constructing the Secure Index: The private cloud prepares data received from the user for privacy-preserving storage. The private cloud constructs a secure index as shown in above figure for keyword search.

proposed pattern hiding scheme

- Encrypting the Data Files: We added a time tag t_f to a linked list node. The time tag infers which update key was used to encrypt the corresponding file and facilitates the search by the date/time of creation of the data. The time tag t_f is in the form of month/day/year
- Hiding the Patterns: The idea is to extend a linked list to contain other keywords in addition to the intended one. Each linked list will contain multiple (but not necessarily same number of) keywords and each keyword

proposed pattern hiding scheme

will appear in multiple (but not the same number of) linked lists

- 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 users data though they are unauthorized to.

Retrieving the Data Files:

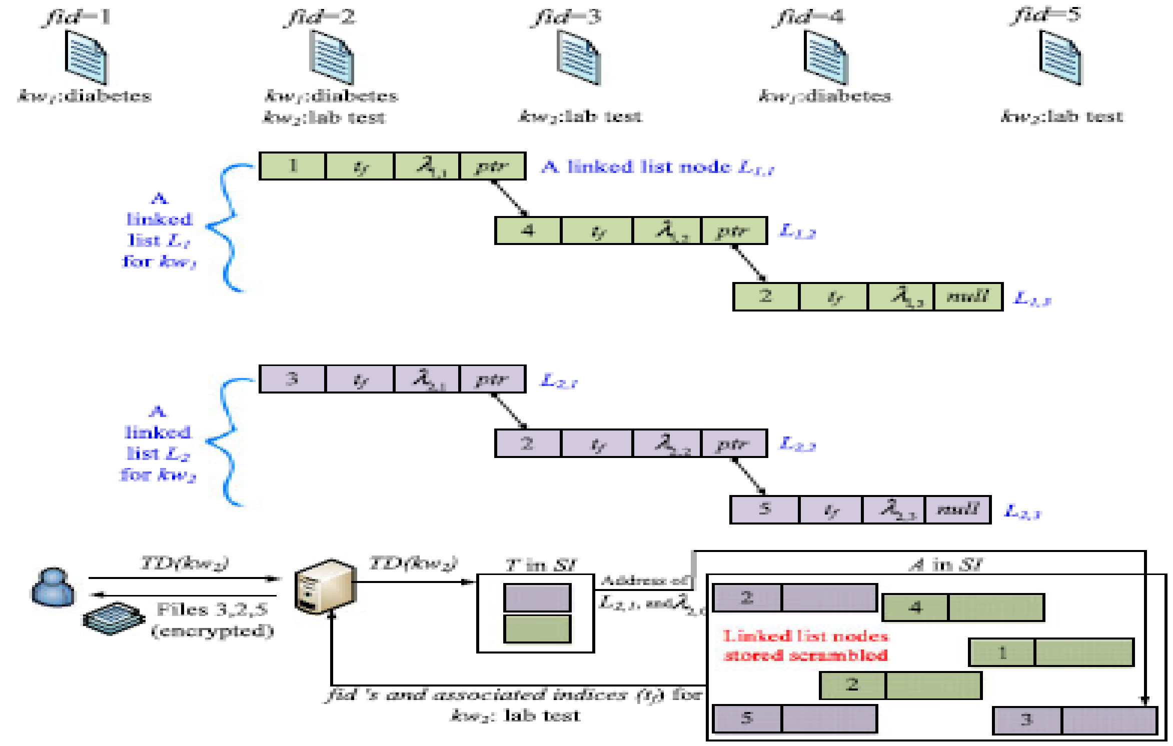


Fig. 4. Example of the construction process of secure index for five files sorted by two keywords, two linked lists each created for a keyword, and a search based on the keyword "lab test."

- The private cloud retrieves the data files upon request on behalf of the user. Suppose files containing "diabetes" are desired

Retrieving the Data Files:

- The private cloud computes a trapdoor for “diabetes” and sends it to the public cloud.
- The public cloud uses trapdoor and computes the address of decrypted link list Li for “diabetes”
- The public cloud will then be able to obtain the addresses and secret keys for all the nodes in this linked list.
- After the whole linked list is decrypted, the time tag is used by the public cloud to determine if a particular file is within

Retrieving the Data Files:

the time range of the request submitted by the private cloud.

- The associated file id's are then used to find the corresponding encrypted files.
- The files and their time tags are finally returned to the private cloud.
- The private cloud regenerates the update keys based on the time tags to decrypt the files.
- Decrypted files are provided to user

Storage and Communication Efficiency

- We analyze the storage and communication efficiency by looking at the storage and communication overheads during data outsourcing and retrieval.
- By analyzing real data, it is found that the storage overhead is linear with the number of outsourced healthcare data files, while the communication overhead can be considered as constant per data request.
- The result indicates that the proposed scheme is efficient as well as scalable..

Computation Efficiency

- While analyzing the computational efficiency of the proposed schemes, Authors concentrated on whether their schemes are efficient when mobile devices are involved, i.e., patients preparing the privacy-preserving storage and EMTs accessing the medical data in emergencies.
- Authors implemented their schemes using Samsung Nexus S smart phones (1-GHz Cortex-A8, 512-MB RAM) and measured the runtime.
- It was found that Roughly, for each access, it takes around 16 s to perform the

Computation Efficiency

required cryptographic computation using the chosen Smartphone and around 0.6 s on the laptop, both of which are acceptable for an efficient retrieval of electronic healthcare records.

Advantages of Proposed System

- The proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the cloud-based data/computation outsourcing paradigm.
- The proposed system has other cryptographic mechanisms for privacy-preserving access of general data stored in a cloud environment.
- The proposed solutions are built on the SaaS model of cloud computing. A software as a service (SaaS) provider provides private cloud services by using the infrastructure of the public cloud providers.

Minimum Hardware Configuration of the proposed system

Processor	:	Intel/AMD
Speed	:	1.1 GHz
RAM	:	256 MB
Hard Disk	:	20 GB
Keyboard	:	Standard Keyboard
Mouse	:	Standard Mouse
Monitor	:	SVGA/LCD

Software Configuration of the proposed system

Operating System	:	Windows
Technology	:	Java and J2EE
Web Technologies	:	HTML, JavaScript, CSS
IDE	:	Eclipse
Web Server	:	Tomcat 6/7
Tool kit	:	Android Phone
Database	:	MySQL 5.5
Java Version	:	JDK 1.6/1.7/1.8

Conclusion

- In this paper, authors proposed to build privacy into mobile health systems with the help of the private cloud.
- They provided a solution for privacy-preserving data storage by integrating existing key management technique for unlinkability, a search and access pattern hiding scheme based on redundancy, and a secure indexing method for privacy-preserving keyword search
- As future work, someone can plan to devise mechanisms that can detect whether user’s health data have been illegally distributed, and identify possible source(s) of leakage

Questions?

Thank you