Cloud - Assisted Mobile - Access of Audited Health Data

Annapureddy Ajay Kumar ¹ & A. Nageswara Rao ²

¹ M.Tech student, Eswar College of Engineering, Narasaraopet, Guntur.
² Asst. Professor & Project Supervisor, Eswar College of Engineering, Narasaraopet, Guntur.

Abstract

The suggested by the secrecy problem, contain the adoption of electronic health secure systems and the wild success of cloud service models, we implement to constitution secrecy into mobile health secure systems with the help of the personal cloud. Our system offers silent characteristics involve effective key management, privacy-preserving data cache, and recovery, especially for retrieval at emergencies, and audit ability for misusing health data.

Specifically, we appliance to merge key management from pseudorandom number generator for unlink ability, a protected indexing method for secure conserved keyword search which hides both search and access patterns based on redundancy, and integrate the concept of aspect based encryption with beginning sign for supply the role-based access control with audit ability to avoid potential misconduct, in both normal and emergency cases.

Keywords—Access control; Audit ability; eHealth; Privacy

I. Introduction

Speed access to health data empower to improved health secure service equipment, make to become better aspect of life, and advice preserving life by helping timely treatment in medical accidents. Anywhere-anytime-accessible electronic health secure systems play a important role in our day to day life.

Services backed personally by mobile devices, such as home care and remote monitoring, allow patients to back to their normal living style and cause minimum break to their daily works. In addition, it somewhat cut down the hospital inhabitancy, allowing patients with more need of in-hospital analysis to be admired.

Although these e-health secure systems are more and more attractive, a large amount of particular data for medical desires are involved, and people start to recognize that they would entirely lose control over their particular information once it enters the cyberspace.

Fig. 1. SaaS service model.

According to the government database, around 8 million patients’ health data was leaked in the last two years. There are good in condition for preservation medical data personal and restrict the access. An employer may make a determination not to hire someone with particular condition. An insurance company may reject to secure life insurance aware the condition report of a patient.

Despite the paramount importance, personal problems are not addressed adequately at the specialized level and efforts to keep health data secure have often fallen short. This is
because protecting security in the cyberspace is somewhat more dispute. Thus, there is an urgent need for the development of viable protocols, architectures, and systems assuring security and privacy to safeguard sensitive & personal digital information. Out patient data safe and secure and computational tasks becomes a popular trend as we enter the cloud computing era. A wildly successful story is that the company’s total claims capture and control (TC3) which provides claim management solutions for healthcare payers such as Medicare payers, insurance companies, municipalities and self-insured employer health plans. TC3 has been using Amazon’s EC2.

Clouds to process the data their patients send in (tens of millions of claims daily) which involve dedicate health data. 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 data faster and more efficiently. The proposed cloud-assisted mobile health networking is inspired by the power, flexibility. The proposed solutions are built on the service model shown in Fig. 1.

A software as a service (SaaS) provider provides private cloud services by using the infrastructure of the public cloud providers (e.g., Amazon, Google). 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 light weight tasks.

Some early works on privacy protection for e-health data concentrate on the framework design [2]–[6], including the demonstration of the significance of privacy for e-health systems, the authentication based on existing wireless infrastructure, the role-based approach for access restrictions, etc. In particular, identity-based encryption (IBE) has been used for enforcing simple role-based cryptographic access control. Among the earliest efforts on e-health privacy, Medical Information Privacy Assurance (MIPA) pointed out the importance and unique challenges of medical information privacy, and 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 facilitate the development of a health information system, in which individuals can actively protect their personal information.

We followed our line of research with other collaborators and summarized the security requirements for e-health systems in. Privacy-preserving health data storage is studied by Sun et al., where patients encrypt their own health data and store it on a third-party server. This work and Searchable Symmetric Encryption (SSE) schemes are most relevant to this paper. Another line of research closely related to this study focuses on cloud-based secure storage and keyword search.

The detailed differences will be described later. The proposed cloud-assisted health data storage addresses the challenges that have not been tackled in the previously stated papers. There is also a large body of research works on privacy preserving authentication, data access, and delegation of access rights in e-health systems, while are most related to our proposed research. Lee and Lee proposed a cryptographic key management solution for health data privacy and security. In their solution, the trusted server is able to access the health data at any time, which could be a privacy threat. The work of Tan et al. is a technical realization of the role-based approach proposed in.

The scheme that failed to achieve privacy protection in the storage server learns which
records are from which patient in order to return the results to a querying doctor. Benaloh et al. proposed the concept of patient-controlled encryption (PCE) such that health-related data are decomposed into a hierarchy of smaller piece of information which will be encrypted using the key which is under the patients’ control.

They provided a symmetric-key PCE for fixed hierarchy, a public-key PCE for fixed hierarchy, and a symmetric-key PCE for flexible hierarchy from RSA. The first public-key PCE for flexible hierarchy from pairings is proposed by Chu et al. [30]. The system of Li et al. [29] utilizes multi authority attribute-based encryption (ABE) proposed by Chase and Chow for fine-grained access control. The system allows break-glass access via the use of “emergency” attributes.

However, it is not clear who will take on the role of issuing such a powerful decryption key corresponding to this attribute in practice. The backup mechanisms in for emergency access rely on someone or something the patient trusts whose availability cannot be guaranteed at all times.

Moreover, the storage privacy proposed in is a weaker form of privacy because it does not hide search and access patterns. The previously stated research works failed to address the challenges in data privacy, we aim to tackle in this paper. Finally, we also remark that there are other cryptographic mechanisms for privacy-preserving access of general data stored in a cloud environment.

II. Performance Evaluation

A. Storage and Communication Efficiency

We analyze the storage and communication efficiency by looking at the storage and communication overheads during data outsourcing and retrieval. The overhead is defined to be any information that serves the purposes of management, security, bookkeeping, etc., but the essential healthcare data or its encryption. For ease of presentation, we list in Table I notations of parameters that we will use in the analysis. The storage overhead is mainly due to the use of Secure Index, which employs linked lists, the lookup table $T$, and an array $A$.

B. Computation Efficiency

In this section, we check the computational efficiency of proposed techniques. Specifically, we are interested in whether our techniques are efficient when mobile devices are involved, i.e., patients preparing the privacy-preserving storage and EMTs accessing the medical data in emergencies.

We implemented our schemes using Samsung Nexus S smart phones (1-GHz Cortex-A8, 512-MB RAM) and measured the runtime. For implementations of IBE and ABE, we used the Java Paring-Based Cryptography Library [42] and used a pairing-friendly type-A 160-bit elliptic curve group. In privacy-preserving storage leveraging patient mobile devices, efficient secret key operations are mainly involved which we will not focus on in the evaluation.

In emergency medical data access leveraging EMT mobile devices, the most costly real-time computation includes IBE decryption and ABE decryption, generating a regular signature on attributes and a partial threshold signature on the access request, and verifying the partial threshold signature from the private cloud.

However, IBE decryption, ABE decryption, and regular signature can be performed once and for all access for the same patient, which is beneficial if the EMT will issue multiple access requests. We still take this cost into account since an EMT is likely to access a patient’s medical data only once in many cases.
We summarize the most costly real-time computation on EMT’s mobile devices in Table IV. The Smartphone we used is not the latest model. The runtime is expected to improve with newer and more powerful models.

For comparison, we also provide in the table the runtime of the same implementation on a laptop (Intel Core i5, 4-GB RAM), which can also be regarded as a mobile device. Roughly, for each access, it takes around 16 s to perform the 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.

### III. Future Work

As a future work, we plan to devise mechanism through which user can communicate with doctors or we can say that face to face communication of users and doctors.

We will also plan to devise mechanisms that can detect whether users’ health data have been illegally distributed, and identify possible source(s) of leakage. In future Mobile health apps exist in a gray zone between medical devices, which are highly regulated, and computer applications, which aren’t regulated much at all. When an app is used to forward the communication between a medical device, such as a blood pressure monitor and a mobile phone that sends data to a tracker office.

### IV. Conclusion

In this paper, we proposed to build an application of mobile health secure System using cloud. Silent features of our health care system are to provide medical camp with their location, provide disease oriented information, provide primary solution to particular disease, and provide hospital locations. This system provides a disease oriented information. This application provides easy access to medical care information anytime and anywhere. We also provide privacy. This system or application is most useful in emergency cases. This system provides the different medical camps with their name and purpose. Our system also provides the nearest hospital location.

### V. References


VI. Authors Profile

Annupreddy Ajay Kumar is a student pursuing MTech(CSE) in Eswar college Of Engineering, Narasaraopet, Guntur.

A. Nageswara Rao M.Tech in Computer Science & Engineering. He is presently working as an Asst. Prof. in Eswar College of Engineering, Narasaraopet, Guntur, India. He is having about 6 years of teaching experience.